School Cyberlaw

PART I

Cyberspeech: First Amendment and Defamation

by David Hostetler

The rapidly developing array of internet and other interactive computer services . . . represent[s] an extraordinary advance in the availability of educational and informational resources to our citizens.

U.S. Congress, 47 U.S.C. § 230(a)(1)

Our inventions are wont to be pretty toys, which distract our attention from serious things. They are but improved means to an unimproved end.

Henry David Thoreau

That technology confronts us with great opportunities and equally great challenges is just as true in public education as it is in other fields. While electronic technology rapidly pervades public school education, the law tags along behind. Old and established rules of law, as well as new rules, are now evolving to address unanticipated issues related to the use of electronic communications in schools. E-mail, Web pages, listservs, and electronic bulletin boards invite new (and more numerous) legal challenges for schools and the people who run them. School officials who understand the law and proceed cautiously when making decisions either to expand or curtail electronic resources and communications will reduce their risk of "cyberliability."

This article, the first of a three-part series on technology law and public schools, addresses issues of First Amendment free speech and defamation raised by use of computers and the Internet by students and school employees. Part II will consider "Cybersafety: Child Protection and Privacy," and Part III will look at "Cybersystems: School Operations and Other General Issues."

The First Amendment

"Congress shall make no law . . . abridging the freedom of speech." So says the First Amendment. In 1982 Chief Justice Warren Burger commented that "[t]he First Amendment . . . must deal with new problems in a changing world."[1] This is even more true today as courts grapple with the meaning of the First Amendment as applied to electronic speech. Commentators have noted that the Internet, like a worldwide soapbox, gives individuals an easily accessible, inexpensive, and expansive arena in which to express their ideas. It therefore confronts school officials with expanding issues of free speech.

Expression by Students

Primary Cases and Principles

It is an oft-quoted principle of law that although the First Amendment rights of students in schools are not equal to those of adults in other public spheres, students do not shed all their free speech rights when they step inside the school building. What does this mean about student electronic expression that is transmitted over school computer lines?

The First Amendment, of course, never protects expression involving defamation, obscenity, child pornography, or speech that threatens (or incites others to) imminent violence or unlawful conduct. Beyond these parameters are several guidelines provided by prior U.S. Supreme Court decisions. In 1969, in *Tinker v. Des Moines Independent Community School District*, the Court upheld the right of students to wear black armbands in school as a way to silently express their opposition to the Vietnam War. In this famous case, the Court established the principle (the *Tinker* standard) that school officials

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. This article is adapted from "School Cyberlaw," Chapter A.9, *Education Law in North Carolina*, ed. Janine Murphy (Chapel Hill: Principals' Executive Program, University of North Carolina, 2004).

1. *See* Board of Educ. et al. v. Pico et al., 457 U.S. 853, 885 (1982).

seeking to restrict noncurricular political expression must be able to forecast that the expression will cause "substantial disruption of or material interference with school activities."[2]

In 1986, in *Bethel School District No. 403 v. Fraser*, the Court upheld the three-day suspension of a student who had made a lewd campaign speech at a school assembly.[3] The decision affirmed a general policy prohibiting "conduct which materially and substantially interferes with the educational process [i.e., the *Tinker* standard] . . .[,] including the use of obscenity, profane language or gestures." In this case, the Court reasoned that the schools also had a prevailing interest in promoting "fundamental" civic values and socially acceptable behavior as well as in protecting students from offensive communications.

In 1988, in *Hazelwood School District v. Kuhlmeier*, the Court upheld the authority of a high school principal to delete from a school-sponsored, student-written newspaper an article about the pregnancies of three unidentified students and an article criticizing a student's father.[4] The Court reasoned that because the newspaper was school-sponsored and part of the curriculum, the principal's actions only needed to be reasonably related to a legitimate pedagogical purpose—in this case, avoiding the impression that the articles were published under the school's imprimatur and preventing disclosure of sensitive information.

"Congress shall make no law . . . abridging the freedom of speech."

These three cases provide the parameters for school officials and courts confronted with cyberspeech issues. Courts differ, however, on when and how to apply them in an electronic context. For example, some courts apply a strict *Tinker* ("substantial disruption") standard, while others apply a hybrid of *Tinker* and other principles (e.g., *Bethel's* permitting sanction of vulgar or uncivil speech). The following section discusses several contexts in which cases have been or are likely to be decided. Except for instances of "off-campus" cyberspeech, all assume that the student in question used school-owned technology.

Forum Analysis: Public, Limited Public, and Nonpublic Forums

When a court reviews a speech restriction, it sometimes considers the context in which the challenged speech occurred to determine the appropriate degree of legal scrutiny to apply. Usually referred to as *forum analysis*, this examination considers a spectrum of different contexts. At one end of the spectrum, the greatest constitutional protection applies to expression in *public forums*, contexts traditionally available for public speech —for example, public parks where individuals are free to speak their mind to anyone who will listen. In such instances, a government speech restriction is subject to strict scrutiny; that is, the restriction must further a compelling governmental interest and use the least-restrictive means to accomplish that interest.

At the other end of the spectrum are nonpublic forums—contexts not traditionally reserved for open expression. Speech in public schools, at least to the extent it occurs in the context of a curricular-related activity (i.e., an activity associated with the school's educational program), is speech in a nonpublic forum. In nonpublic forums, the government may impose a speech restriction as long as it is rational; that is, as long as the restriction is reasonably related to a legitimate governmental objective and does not discriminate on the basis of the viewpoint expressed by speech that is appropriate to the purpose(s) of the forum.

Along the spectrum between public and nonpublic forums are *limited public forums* (sometimes referred to as *designated forums*) that are created by the government for a special public purpose. In such forums, the government may impose reasonable speech restrictions that are subject to lesser legal scrutiny if they reasonably relate to the forum's legitimate purpose. Restrictions on particular viewpoint-related speech whose content fits the particular purpose for which the forum was created, however, are subject to strict scrutiny; any such restriction must be narrowly tailored to further a compelling governmental interest.

Whether and how forum analysis applies to electronic communications is not entirely clear. The 2003 case of *U.S. v. American Library Association*[5] involved the constitutionality of the federal Children's Internet Protection Act (CIPA), which requires federally funded public library computers to be fitted, in essence, with Internet filters.[6] The U.S. Supreme Court ruled that public library Internet access (due to its recent emergence) has no historical tradition of open speech and is therefore neither a public forum nor a designated (or limited) public forum. According to the Court, the government may impose speech restrictions (in the form of Internet filters) on public library computers according to the "reasonableness" standards applied to nonpublic forums—that is, restrictions that are reasonably related to a legitimate governmental purpose. It would seem that similar logic would apply to public school computers.

In a case decided before *American Library Association*, a Tennessee newspaper publisher asked a city to add a link from its Web page to the newspaper's Web page.[7] The city denied

2. Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 514 (1969).
3. Bethel Sch. Dist. v. Fraser, 478 U.S. 675, 678 (1986).
4. 484 U.S. 260 (1988).
5. 123 S. Ct. 2297 (2003).
6. Pub. L. No. 106-554.
7. The Putnam Pit, Inc. et al. v. City of Cookeville, 23 F. Supp. 2d 822, 832 (M.D. Tenn. 1998).

the request, basing its decision on a city policy that limited Web links to entities that "promote the economic welfare, tourism and industry" of the city. The court rejected the plaintiff's argument that the Web page was a public forum and, therefore, that the city's restriction was subject to strict scrutiny: "[I]t is clear that unlike public streets and parks, web pages on the internet have not by long tradition or government fiat been devoted to assembly and debate; nor has the City's web page immemorially been held in trust for the use of the public."[8] On appeal, the Sixth Circuit Court of Appeals agreed with the district court that the Web page was not a public forum.[9]

In certain circumstances, school facilities or other nonpublic forums have been transformed, sometimes inadvertently, into public or limited public forums when school authorities, by "policy or practice," opened those facilities "for indiscriminate use by the general public, or by some segment of the public, such as student organizations."[10] For example, a Wisconsin public school district opened its computer lab to the public after school hours (thus converting it into something like a public library computer lab). A high school student who used one of the computers during this after-school period to search Web sites about witchcraft was prohibited from doing so by the lab supervisor. After the student filed an administrative complaint with the state department of public instruction, the school system, presumably recognizing its potential First Amendment liability, relented.[11]

In *Loving v. Boren*, an Oklahoma University (OU) professor sued the university's president because the university refused access to the university's computer news servers to certain news groups believed to propagate obscene material.[12] The restrictions were prompted by the university's effort to avoid possible criminal penalties under a state law prohibiting distribution of obscene materials. Just before the case went to trial, the university established a new, two-tiered news server access scheme: one tier prevented users from accessing the news groups in question; the second tier allowed unlimited access by adults who consented to the terms of use and used the server only for educational and research purposes.

Although the court decided the case primarily on technical grounds, it also considered whether the news server was a public forum for First Amendment purposes.

> The OU computer and Internet services do not constitute a public forum. There was no evidence at trial that the facilities have ever been open to the general public or used for public communication. The state, no less than a private owner of property, has the right to preserve the property under its control for the use to which it is lawfully dedicated. In this case, the OU computer and Internet services are lawfully dedicated to academic and research uses. Within these uses, access by an adult is plenary [i.e., unrestricted].[13]

School officials must be cautiously aware that when they create Web pages, discussion groups, e-mail lists, etc., they may be creating a limited public forum. To preserve the intended purposes and limits of the particular electronic forum, officials should define and communicate clearly the educational purpose of the service provided. For instance, a school Web page policy might permit the school's Web page to contain links to the Web pages of extracurricular student groups that promote the school's educational program or provide educationally related social benefits. Under the First Amendment, school officials could therefore justifiably exclude a link to a Web page that is not school related—for example, a link to a page promoting a student's personal business or other interests.

Electronic Distribution of Noncurricular Literature

Individuals and groups often wish to distribute literature on school property. Such distribution sometimes requires prior administrative approval and is permitted only at designated locations such as school lobbies, hallways, or exits. The same groups may wish to distribute organizational literature or opinions via school-supported e-mail accounts, Web pages, and electronic discussion lists.

First Amendment law governing the distribution of literature is unsettled—especially in regard to electronic distribution. It is clear that school officials may prohibit distribution of material that creates a foreseeable risk of substantial disruption of or material interference with its educational mission, promotes unlawful or harmful activities, or is obscene, indecent, or defamatory. Beyond these parameters, however, administrators must examine and decide whether and how their current practices and policies governing traditional means of distribution should extend to electronic distribution.

First, school officials need to articulate the purpose of the electronic media they are creating as narrowly as possible to fit its intended purpose. For example, a lobby bulletin board may be designated for use only by teachers and only for the purpose of posting class assignments. Similarly, a particular e-mail address or Web site may be designated only for communications between parents and school administrators about school-related matters.

---

8. *Id*. at 829.

9. The Putnam Pit, Inc. et al. v. City of Cookeville, 221 F.3d 834 (6th Cir. 2000). When the case was sent back to the district court, the jury ruled that the newspaper did not meet the city's criteria for linking to other Web sites. This decision was affirmed on appeal. No. 01-6599, 2003 U.S. App. LEXIS 17775 (August 20, 2003) (opinion subject to limited-citation rule).

10. *Hazelwood*, 484 U.S. at 267.

11. "Barring Student's Access to Witchcraft Site Brings Wisconsin District Toil and Trouble," *eSchool News Online*, May 1999, available to subscribers at http://www.eschoolnews.com/news/browse.cfm.

12. 956 F. Supp. 953 (W.D. Okla 1997), *aff'd.*, 133 F.3d 771 (10th Cir. 1998).

13. *Id.* at 955.

In the 1998 case, *Boucher v. School Board of the School District of Greenfield*, a federal court of appeals upheld a Wisconsin school system's expulsion of high school junior Justin Boucher for publishing an article entitled "So You Want To Be a Hacker."[14] Boucher wrote the article at home but published it in an underground newspaper that was distributed in school bathrooms and in the cafeteria. (The opinion does not indicate who was responsible for publishing or distributing the paper.) Boucher's stated purpose was to "ruffle a few feathers and jump-start some to action." He wrote that he wished to "tell everyone how to hack the school['s] . . . computers" and went on to explain, for example, how to "see a list of every file on the [school's] computer," including student and teacher log-in names, how to break into the system's computer programs, how to view a list of current users, and how to avoid getting caught.

School officials suspended Boucher for fifteen days at the end of the school year. Following a hearing during the summer, the school board also expelled him for the next school year, finding that the article had "endangered school property" in violation of local policy and had disclosed access codes in violation of Wisconsin state law.

Boucher sued the school system, alleging it violated his free speech rights.[15] A federal trial court granted Boucher's request for a preliminary injunction to block the expulsion until the case had been fully tried. The Seventh Circuit Court of Appeals, based on *Tinker's* "foreseeable disruption" standard, however, overturned the injunction. Said the Seventh Circuit,

> [t]he utter defeat of the Board's disciplinary efforts when confronted by a self-proclaimed "hacker" is clearly a substantial harm. . . . The Supreme Court "has repeatedly emphasized the need for affirming the comprehensive authority of the States and of school officials, consistent with fundamental constitutional safeguards, to prescribe and control conduct in the schools. . . . Without first establishing discipline and maintaining order, teachers cannot begin to educate their students." We think that, in this procedural posture, it is enough to show that school discipline, undertaken reasonably and in good faith to protect the school's vital interest, is being undermined.[16]

Off-Campus Expression

Students sometimes publish cyber news Web pages (like "underground" newspapers) that contain expression normally avoided or prohibited on school grounds.[17] Under the First Amendment, school officials have very limited authority to regulate such expression when it occurs in a private context off of school grounds unless they can reasonably foresee that the expression will threaten or cause harm or disruption to people or property associated with the school system.

Thus far, most of such cases have been decided or resolved in favor of students. For example, in *Beussink v. Woodland RIV School District*, a high school junior posted a Web page from his home computer containing vulgar criticisms about his high school principal, teachers, and the school's Web page.[18] There was no evidence that Beussink ever used a school computer to create or work on his Web page. Eventually, a fellow student, apparently to get Beussink in trouble, opened the Web page on a school computer and showed it to the computer teacher. After viewing the page, the principal suspended Beussink for ten days and required him to modify or remove the Web page. There was no clear evidence that the page had created any substantial disruption at the school, even though the computer teacher allowed some students to access it and discussed it with them, possibly as an object lesson.

Beussink's ten-day suspension (which the school counted as an unexcused absence) contributed to failing grades and jeopardized his ability to graduate on time. He sued to enjoin the school district from carrying out its policy of lowering grades for unexcused absences.

To issue a preliminary injunction before the case's final outcome, the court needed to determine whether Beussink was likely to succeed in his First Amendment claim. Applying the *Tinker* "substantial disruption" standard, the court ruled that the suspension was a result of the principal's abrupt reaction to the Web page and not of any actual or foreseeable disruption. The court also ruled that Beussink's interests in obtaining the injunction outweighed those of the school in preventing it and that the injunction best served the public interest: "[T]he public interest is not only served by allowing Beussink's message to be free from censure, but also by giving the students at Woodland High School this opportunity to see the protections of the United States Constitution and the Bill of Rights at work."[19]

In a similar case, a Washington federal district court restrained a school system from suspending a high school student for five days after the student posted "mock obituaries" of his friends on a personal Web page.[20] Visitors (mostly other students) to the Web page were invited to vote on who

14. 134 F.3d 821, 822 (7th Cir. 1998).

15. *Id*. Boucher also sought a preliminary injunction to prevent the school system from enforcing its decision pending the outcome of the case. In such instances, the court must predict the likelihood that the plaintiff will prevail in the trial; it must also weigh the degree of potential harm that would be caused to each party by the issuance or nonissuance of the injunction.

16. *Id*. at 827 (quoting *Tinker*, 393 U.S. at 507).

17. See, for example, "Channel Zero (The Underground Newspaper Webring)," which contains an extensive listing of such underground news pages, http://www.oblivion.net/~ugpapers/ (last visited June 18, 2003).

18. 30 F. Supp. 2d 1175 (E.D. Mo. 1998).

19. *Id*. at 1182.

20. Emmett v. Kent Sch. Dist. No. 415, 92 F. Supp. 2d 1088 (W.D. Wa. 2000).

should "die" next—that is, which student should be the subject of the next mock obituary. The Web page included disclaimers that the page was for entertainment purposes only. Although administrators had been aware of the site, they did not impose the suspension until after it became public knowledge through a televised news report that erroneously characterized the page as a "hit list."

Because the speech occurred off school property, and because school administrators presented no evidence that the obituaries and voting on the Web site were intended to, or actually did, threaten anyone, the judge determined that the student was likely to prevail in his lawsuit against the school.

In *Coy v. North Canton City Schools Board of Education*, Jon Coy, an Ohio middle school student, created a Web site on his home computer containing a section entitled "losers" that derided several fellow students.[21] The site contained profanity, pictures of boys giving the "finger," and, in the court's opinion, a "depressingly high number of spelling and grammatical errors."

Following a student tip, the principal viewed the site and then had the school technology coordinator monitor Coy's in-school computer use during computer class. This monitoring showed that Coy accessed his own Web site during class. The principal suspended Coy for four days based on three different student conduct code provisions prohibiting obscenity, disobedience to school rules, and "inappropriate behavior." The school board upheld the suspension as well as the superintendent's imposition of a suspended eighty-day expulsion (i.e., Coy was permitted to be at school but was subject to expulsion for any subsequent violation of school rules). School officials also initiated a police investigation and requested that the Internet service provider (ISP) curtail Coy's Internet access.

Coy sued. The school district argued that it had disciplined Coy for displaying vulgar material at school and for violating the school's student conduct policy, not for creating the Web site. Both parties sought summary judgment (i.e., a ruling of law, without a trial, based on the alleged facts).

The court first determined that the *Tinker* (substantial disruption) standard applied to the case. The court stated that the school could discipline Coy for accessing an unauthorized Web site as long as the facts showed that school officials were motivated by a desire to uphold the conduct code rather than by dislike of the Web site's content. Coy's second claim challenged the constitutionality of the code of student conduct on the basis that it was overbroad and vague. The court held that the rules prohibiting obscenity and disobedience to school officials were not unconstitutional on their face but might be unconstitutional as applied if school officials imposed the discipline due to a desire to close down the offensive Web site. The court did strike down, for vagueness, the part of the policy prohibiting "any action or behavior judged by school officials to be inappropriate."[22] The court denied both parties' summary judgment motions because the remaining factual issues required a jury verdict.

In a 2002 Detroit case, *Mahaffey v. Aldrich*, high school officials suspended a student after he admitted to contributing to a Web site entitled "Satan's Webpage."[23] The site, which belonged to one of his friends, included the names of people the creator wished to die, as well as a section titled "Satan's Mission of the Week," which instructed viewers to "stab someone for no reason then set them on fire and then throw them off of a cliff." The school suspended the plaintiff indefinitely pending a school board hearing. The hearing was cancelled when school board members learned that the student was enrolled in a different school. The student, however, requested a subsequent hearing. The board then met and ruled on the case but neglected to notify the student of its findings for more than a month. The student sued the school, claiming that the suspension violated his free speech rights and that the delayed hearing and notice violated his due process rights.

The district court ruled in favor of the plaintiff on his free speech claim.[24] The court determined there was little evidence that the plaintiff's conduct (contributing to the Web site) occurred on school grounds (the school never investigated whether the plaintiff actually used school computers) or that the Web site affected the day-to-day operations of the school. Furthermore, the court ruled that the contents of the Web site did not constitute genuine threats against any particular person.

In a Pennsylvania case, a student and his parents brought an action against a school district after the student was disciplined under a handbook policy that prohibited speech that was "abusive, harassment, inappropriate, or offensive."[25] The student was punished for posting critical and derogatory comments about an opposing school's volleyball team and its students on a message board. One message, for example, referred to a member of the volleyball team and his mother: "You're no good and your mom's a bad art teacher. . . . My mom can teach better than Bemis' mom." Another message stated that "the purple pansies are in for the surprise of their lives." Of the four messages sent, one was transmitted from a computer at school and three others were sent from the student's home computer.

The court found the handbook policy to be constitutionally overbroad because it was not limited to (1) speech that substantially disrupted school operations and (2) speech occurring

21. 205 F. Supp. 2d 791 (N.D. Ohio 2002).

22. *Id.* at 802.

23. 236 F. Supp. 2d 779 (E.D. Mich. 2002).

24. *Id.*

25. Flaherty v. Keystone Oaks Sch. Dist., 247 F. Supp. 2d 698, (W.D. Pa. 2003).

on school grounds or transmitted through school computers. The policy was also ruled too vague because the student handbook did not define the terms "abusive," "harassment," "inappropriate," or "offensive," thereby creating an unreasonable risk of arbitrary enforcement.

Several of the cases involving the following actions by schools (as reported in the news) were similarly decided or settled in favor of students who posted controversial personal Web pages:[26]

- revocation of a student's National Merit scholarship for posting a Web page that contained a parody of the school,
- suspension of an Ohio student for posting a Web page containing an insult to a band teacher,
- suspension of a student for posting a Web page entitled "Stow High School Sucks,"
- exclusion of a student from a school computer lab for posting a mock Web page entitled "Chihuahua Haters of the World,"
- suspension of a student for ten days for posting a Web page containing a statement that the assistant principal had "the personality of sour milk,"
- suspension of a high school student for posting a Web page containing altered electronic photographs of a school administrator appearing in Viagra ads and engaging in sordid behavior, and
- suspension of a student for creating a "top-ten" e-mail list that vilified the school's athletic director. (An unidentified student reformatted the list and passed it around at school.)[27]

The clear lesson for school administrators is that students can be disciplined for off-campus electronic expression only on the basis of an actual or foreseeable disruption of school activities or harm threatened against individuals or property —not because the expression is simply disrespectful, rude, or offensive. Officials should avoid hasty disciplinary actions and be careful to document efforts to determine the extent, if any, to which the material was created or appeared on school computers and the extent of foreseeable or actual threat to school operations, property, or safety.

However, courts have supported disciplinary action for private Web pages in some instances. In 2002, in *J.S. v. Bethlehem Area School District*, the Pennsylvania Supreme Court upheld the expulsion of a fourteen-year-old student who posted a "Teacher Sux" Web site.[28] The site contained "derogatory, profane, offensive and threatening comments," primarily about the student's algebra teacher and the principal. One page began, "Why Should She Die?" (referring to the teacher) and invited readers to "take a look at the diagram and the reasons I give, then give me $20 to help pay for the hit man." That page included images of the teacher being decapitated (with blood dripping from her neck) and "morphing" into Adolph Hitler. Some pages urged that the teacher be fired because of her physique and disposition, referred to her as a "b____" or "stupid b____," and contained a picture of the teacher as a witch.[29]

Believing the threats to be serious, the principal informed faculty of a problem (without disclosing the specifics) and notified local police and the Federal Bureau of Investigation. (Neither agency filed charges after investigating the incident and learning that J.S. was the Web site's author.) On his own initiative, J.S. removed the Web site within a week after the principal learned about the site.

The teacher, frightened by the threats, became ill and suffered numerous side effects (sleeplessness, stress and anxiety, loss of weight) and took a medical leave of absence for the remainder of the school year (requiring three different substitute teachers, a matter of concern to parents).

The evidence showed that J.S., at least once, opened the Web site on a school computer and showed a classmate. Once other students and staff became aware of it, they, too, accessed the site and it became the "hot" topic of conversation. The principal testified that, as a result of the site's notoriety, morale at the school was "worse than anything he had witnessed" in his forty-year professional career, comparing its effect to the death of a student or staff member.

During the remainder of the school year, J.S. continued attending classes and participating in extracurricular events. The school board eventually expelled him prior to the resumption of the next school year. The board concluded that (1) the statement "Why Should She Die?" and "give me $20 to help pay for the hitman" constituted a threat in violation of school policy and resulted in harm to the teacher; and (2) other statements regarding the principal and teacher constituted harassment of and disrespect toward a teacher and principal, resulting in harm to the health, safety, and welfare of the school community.[30]

In its analysis, the court addressed two primary issues: (1) whether the Web site posed an "actual threat" of harm; and (2) even if no threat existed, whether the site caused a sub-

---

26. "Teen's Free Speech Extends to Cyberspace," S*t. Louis Post-Dispatch*, January 3, 1999; Dennis Pierce, "Banned Student Newspaper Stories Resurface on Internet: Too Hot for School Newspapers, Inflammatory Student Writing Finding New Audiences Online," *eSchool News online*, May 1998, available to subscribers at http://www.eschoolnews.com/news/browse.cfm; "Web Speech Is Free Speech, Judge Says," *American School Board Journal*, September 2000.

27. Killion v. Franklin Reg. Sch. Dist., 136 F. Supp. 2d 446 (W.D. Pa. 2001).

28. 807 A.2d 847 (Pa. 2002).

29. *Id.* at 851.

30. *Id.* at 852.

stantial disruption to the school community or otherwise invaded the rights of others.[31]

On the first issue, the court determined that no actual threat existed. (A concurring judge disagreed on this point.) Despite the physical and emotional effects of the Web site on the teacher, the court noted that others did not consider it threatening and that J.S. had been permitted to remain in school.

> We believe that the Web site, taken as a whole, was a sophomoric, crude, highly offensive and perhaps misguided attempt at humor or parody. . . .
>
> [W]e do not belittle the harm that [the teacher] has suffered. Moreover, the Court of Appeals for the Ninth Circuit has specifically noted that school officials are justified, given the modern rash of violent crimes in school settings, in taking very seriously student threats against faculty or other students. We too appreciate that in schools today violence is unfortunately too common and the horrific events at Columbine High School, Colorado remain fresh in the country's mind. However, we find that that the speech at issue does not rise to the level of a true threat. Distasteful and even highly offensive communication does not necessarily fall from First Amendment protection as a true threat simply because of its objectionable nature. [32]

The court then moved to the issue of substantial disruption, noting the tension between student First Amendment rights and the need for schools to maintain order and discipline. It also acknowledged the difficulty of applying pre-Internet student First Amendment jurisprudence (i.e., the *Tinker*, *Bethel*, and *Hazelwood* cases) to cases involving electronic communications: "[T]he advent of the Internet has complicated analysis of restrictions on speech. . . . Indeed, *Tinker's* simple armband, worn silently and brought into a Des Moines, Iowa classroom, has been replaced by J.S.'s complex multi-media Web site, accessible to fellow students, teachers, and the world."[33]

The court's analysis hinged, in part, on whether the speech in question should be classified as on-campus speech or off-campus speech (the former being subject to greater school restriction and the latter subject only to *Tinker's* substantial disruption standard). The court concluded the Web site was on-campus speech because J.S. had accessed it on campus and "inspired" other students and staff to do so. Said the court, "We hold that where speech that is aimed at a specific school and/or its personnel is brought onto the school campus or accessed at school by its originator, the speech will be considered on-campus speech."[34]

Following this determination, the court had to decide how to apply Supreme Court precedent. J.S.'s Web site, according to the court, "straddles the political speech in *Tinker*, and the lewd and offensive speech expressed at an official school assembly in *Fraser*."[35] Relying most heavily on *Tinker*, the court concluded that the Web site did substantially disrupt the school community. It was the "hot" topic of conversation among students and staff; J.S.'s algebra teacher missed the remainder of the school year, requiring the school to use three substitute teachers—a matter of concern to parents. School morale declined; and some students had to receive counseling.[36]

School officials may have other practical remedies for dealing with private Web pages containing offensive but constitutionally protected speech. For example, one news account reported that in Missouri an Internet service provider (ISP) was willing, under its user agreement, to shut down a student's personal Web site, which rated the looks and sex appeal of students and teachers at his middle school.[37] Notifying the student's parents of their child's Internet exploits also may yield good results if the parents are willing to impose their own (sometimes tougher) private discipline.

If threats are made to students or school personnel on private Web pages or through other electronic means, administrators should report the threats to law enforcement authorities and encourage students to report to school officials. A Colorado student who received an e-mail message in which the sender threatened to "finish what begun" [*sic*] at Columbine reported the message to school officials, who shut down the high school for two days. Law enforcement authorities tracked the source of the e-mail through the records of the Internet service provider. The sender, an eighteen-year-old Florida resident, subsequently pleaded guilty to criminal charges.[38]

In Pennsylvania, a teacher sued her employer over a "secret assassination plan" that was allegedly posted by a student on the Internet. (The teacher stated that she filed the lawsuit because the school did not do enough to discipline the boy, considering the seriousness of the threat.[39]) After learning of

31. *Id*. at 856–57.

32. *Id*. at 860 (citing Lovell v. Poway Unified Sch. Dist., 90 F.3d 367, 373 [9th Cir. 1996]).

33. *J.S.*, 807 A.2d 864.

34. *Id*. at 865.

35. *Id*. at 866.

36. *Id*. at 869.

37. Dennis Pierce, "ACLU Hits Missouri School District with Internet Free-Speech Lawsuit: Student Suspended over Web Site Content," *eSchool News online,* Oct. 1998, available to subscribers at http://www.eschoolnews.com/news/browse.cfm.

38. "Teenager Pleads Guilty to E-mailed Columbine Threat," *Raleigh News and Observer*, February 10, 2000.

39. www.USAToday.com, April 29, 2003.

the threat, the principal suspended the student for three days and referred the matter to the police. The police filed charges against the boy for making terrorist threats and for electronic harassment.

School systems or individuals subjected to threatening electronic communications might wish, like the teacher mentioned above, to file criminal charges or, in some instances, attempt to recover damages through civil actions.[40]

Restricting Internet Access

The U.S. Supreme Court has compared the Internet to a "vast library including millions of readily available and indexed publications," the content of which "is as diverse as human thought."[41] To minimize the risk of students perusing the more sordid resources of this vast library, many school systems restrict Internet access by relying on filtering software, acceptable-use policies (AUPs), or other means. When taking such actions, school officials must be conscious of the need to balance competing legal concerns between, on the one hand, potential liability when students are exposed to threatening or otherwise harmful materials on school equipment and, on the other, violation of First Amendment rights resulting from excessive access restrictions not motivated by legitimate educational reasons.[42]

The extent to which school officials may restrict student Internet access under the First Amendment is not clear due to the sparse case law. Several court cases, however, offer some guidance.

In 1982, in *Board of Education v. Pico*, the U.S. Supreme Court addressed the issue of whether the First Amendment limits school boards' discretion to remove books from high school and junior high school libraries.[43] The board involved had ordered the removal from school libraries of certain books one board member characterized as "anti-American, anti-Christian, anti-Semitic, and just plain filthy."[44] The Court, in a plurality opinion, held that if the board acted primarily to suppress unpopular social ideas rather than because of a legitimate concern for "educational suitability," it had violated the First Amendment. The Court remanded the case to the trial court for a determination of the board's motivations.

Pico's application to Internet access restrictions in schools remains somewhat unclear. The Court, however, did enunciate several principles having clear implications for Internet restriction.[45] First, the right to speak freely implies a corollary right of access to information.

> "The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers." . . . In sum, just 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 and effective participation in the pluralistic, often contentious society in which they will soon be adult members.[46]

Second, a student has broader First Amendment access rights in the school library than in a teacher-controlled classroom; the library and, by implication, the library's Internet resources provide greater opportunity for self-directed and voluntary learning.

> "[S]tudents must always remain free to inquire, to study and to evaluate, to gain new maturity and understanding." The school library is the principal locus of such freedom. . . . [I]n the school library "a student can literally explore the unknown, and discover areas of interest and thought not covered by the prescribed curriculum. . . . [The] student learns that a library is a place to test or expand upon ideas presented to him, in or out of the classroom."[47]

Finally, the Court acknowledged that school boards have "inculcative" discretion to select or reject, based on communi-

---

40. In a civil action filed in Indiana state court on August 6, 1999, several schoolteachers filed claims (e.g., defamation and intentional infliction of emotional distress) against a student who posted a private Web page suggesting that the teachers were devil worshippers. The site allegedly included satanic symbols, listed the names of eleven school district employees alleged to be devil worshippers, and encouraged student readers to tell teachers that they knew of their "secret" and to "laugh in their faces." The on-line nickname for the site was "tyme-2-dye." "Teachers Accused of Devil Worship Sue Student," *School Law News*, August 20, 1999.

Information on this and related issues for children, parents, administrators, teachers, and other concerned individuals can be accessed at a U.S. Justice Department Web site, www.cybercrime.gov.

41. Reno et al. v. ACLU et al., 521 U.S. 844, 852 (1997).

42. Administrators previously erred on the side of avoiding liability for student harm. *See* Glenn Kubota, "Comment: Public School Usage of Internet Filtering Software: Book Banning Reincarnated?" *Loyola of Los Angeles Entertainment Law Journal* 17 (1997): 687, 704 n.144.

43. 457 U.S. 853, 855–56 (1982).

44. *Id.* at 856 n.3. The books were *Slaughterhouse Five* by Kurt Vonnegut Jr.; *The Naked Ape* by Desmond Morris; *Down These Mean Streets* by Piri Thomas; *Best Short Stories of Negro Writers*, edited by Langston Hughes; *Go Ask Alice* (author unknown); *Laughing Boy* by Oliver LaFarge; *Black Boy* by Richard Wright; *A Hero Ain't Nothin' But a Sandwich* by Alice Childress; *Soul on Ice* by Eldridge Cleaver; and *A Reader for Writers*, edited by Jerome Archer. An appendix to the case quotes specific excerpts from the books containing the alleged sexually lewd and profane language.

45. Predicting how courts will apply these principles is complicated by the fact that the reasoning in *Pico* was not adopted by a majority of the Court's justices and the fact that the case was decided almost twenty years ago.

46. *Pico*, 457 U.S. at 867 (quoting Lamont v. Postmaster General, 381 U.S. 301, 308 [1965]).

47. *Id.* at 868–69 (quoting Keyishian v. Board of Regents, 385 U.S. 589 [1967] and Right to Read Defense Comm. v. Sch. Comm., 454 F. Supp. 703, 715 [Mass. 1978]).

ty values, materials that are age-appropriate. Based on this principle, it is likely that courts in the future will examine Internet access restrictions, when challenged, primarily according to whether or not the restrictions are motivated by concern for educational suitability.

It is important to note that the Court in *Pico* explicitly confined its ruling to the removal of books already in the library collection, not to decisions about whether and what to add to a collection.[48] Implicitly, then, a board may exercise more discretion to limit Internet access at its inception than to curtail access previously granted.

In 2003 a challenge to application of the Children's Internet Protection Act to public libraries (discussed above, p. 2) was brought by a group of libraries, Web publishers, and civil liberties groups.[49] These entities argued that the filters that block access to pornography and other materials deemed harmful to children forced libraries to violate adult patrons' free speech rights of access to constitutionally protected materials. It is worth noting several key principles and considerations regarding restrictions on Internet access discussed in this Supreme Court opinion.

First, the Court pointed out, public libraries have no tradition of making sexually graphic materials available to patrons. Requiring them to do so, therefore, would be contrary to their historical mode of operation. Second, the Court ruled that public library Internet access (because of its limited history) is neither a public forum nor a designated (or limited) public forum. (See above, pp. 2–3, for discussion of forum analysis.) Consequently, a decision to restrict Internet access based on content is not subject to strict scrutiny (which would require the government to have a compelling purpose behind the restriction and to adopt the least-restrictive means of accomplishing that purpose). Third, "[t]o fulfill their traditional missions of facilitating learning and cultural enrichment, public libraries must have broad discretion to decide what material to provide to their patrons."[50]

The Court also pointed to the impractability of applying strict scrutiny to libraries' Internet access.

> [B]ecause of the vast quantity of material on the Internet and the rapid pace at which it changes, libraries cannot possibly segregate, item by item, all the Internet material that is appropriate for inclusion from all that is not. While a library could limit its Internet collection to just those sites it found worthwhile, it could do so only at the cost of excluding an enormous amount of valuable information that it lacks the capacity to review. Given that tradeoff, it is entirely reasonable for public libraries to reject that approach and instead exclude certain categories of content, without making individualized judgments that everything made available has requisite and appropriate quality. Concerns over filtering software's tendency to erroneously "overblock" access to constitutionally protected speech that falls outside the categories software user's intend to block are dispelled by the ease with which patrons may have the filtering software disabled.[51]

In an earlier case, *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*,[52] a Virginia federal district court relied heavily on *Pico*, thus confirming the likelihood that *Pico's* ruling and analysis (focusing on free access to ideas and educational suitability) will inform future school free speech Internet-access cases. In *Loudoun*, the court ruled against a public library that had installed filters on its computers on the grounds that a less-restrictive means could have accomplished the library's intent to avoid sexual harassment.

Together, the cases discussed above support the following recommendations for school officials:

- Make Internet access decisions cautiously and with an awareness of their legal significance. Determine, for example, whether a decision will create new and substantial risks of liability under the First Amendment.
- Decide if and to what extent providing "voluntary" Internet uses (those not required by the curriculum) is worth the legal consequences. (Subsequent decisions to curtail access to resources previously available to students are more likely to be subject to First Amendment challenges.)
- Carefully tailor acceptable-use policies (AUPs) to withstand First Amendment scrutiny; for instance, be reasonably specific and clear as to what is permissible and what is prohibited. Also, choose, monitor, and update any filtering software (if used) to ensure that it accomplishes its intended purposes to a reasonable degree. (For instance, a filtering system that blocks material not intended to be blocked could lead to *Pico*-like liability for curtailing legitimate access.)
- Base Internet-access restrictions solely on reasons of educational suitability and not on an intent to suppress unpopular social ideas. Develop supporting documentation to substantiate the motivations behind Internet access decisions.

48. *Id*. at 871–72.
49. United States v. American Library Association, 123 S. Ct. 2297 (2003).
50. *Id*. at 2304.
51. *Id*. at 2306.
52. 2 F. Supp. 2d 783 (E.D. Va. 1998), summary judgment granted, 24 F. Supp. 2d 552 (E.D. Va. 1998).

- Closely tailor Internet access restrictions to the context (e.g., student ages) and purposes for which the access is provided; provide clear notice of standards, consequences, and procedures for use or abuse of such access.

Employee First Amendment Rights

In the context of cyberspeech, First Amendment issues involving school employees are most likely to entail the issue of freedom to communicate on school-owned computers.

First Amendment Analysis and Recent Case Law

Free speech cases involving government employees normally involve a two-step analysis to determine whether the speech in question is protected. First, the speech at issue must involve a public concern. To determine this, a court considers the content, context, and form of the speech. For example, does the speech address a social, political, or other public interest, and does it relate to the speaker's role primarily as a citizen or primarily as an employee? If the speech does not involve a matter of public concern, it is not protected. If the speech does involve a matter of public concern, the court considers the second step of the analysis: balancing the employee's interests as a citizen to comment on matters of public concern against the state's interest in promoting "an appropriate operation of the workplace."[53]

One of the few federal appellate cases involving school cyberspeech was decided in the Fourth Circuit, which has jurisdiction over North Carolina. *Urofsky v. Gilmore* involved a Virginia statute that prohibited state employees from accessing sexually explicit materials on state-owned computers without department approval.[54] Six Virginia public university professors sued, claiming that the statute violated their First Amendment rights to perform their academic duties. For example, the lead plaintiff, Melvin Urofsky, alleged that he decided not to assign an on-line research project on indecency law because he feared he would be unable to verify his students' work without violating the law. Another instructor claimed the law hindered his access to sexually explicit poetry related to his study of Victorian poets. Several plaintiffs felt restrained from conducting research on human sexuality. (There was no evidence that any of the professors sought a departmental waiver from the law.)

The plaintiffs prevailed at trial in district court, but a three-judge panel of the Fourth Circuit reversed the ruling on the grounds that Internet access on government computers does not involve a matter of public concern. The case was reheard *en banc* by the Fourth Circuit (i.e., by the entire panel of Fourth Circuit judges).[55]

A majority of judges held in favor of the state on the grounds that the speech in question (i.e., work-related access to the Internet) presented no issue of public concern because the speech pertained to the plaintiffs' roles as employees, not as citizens. This majority also ruled that, to the extent the U.S. Supreme Court has recognized a free speech right of academic freedom, such right resides with the institution, not with an individual teacher: "It cannot be doubted that in order to pursue its legitimate goals effectively, the state must retain the ability to control the manner in which its employees discharge their duties and to direct its employees to undertake the responsibilities of their positions in a specified way."[56]

Chief Judge Wilkinson concurred with the decision on the grounds that, though the speech involved a public concern, the state's interests should prevail over the plaintiffs.' But he criticized the majority for simplistically overemphasizing the work-related nature of the speech and for ignoring the public concern presented by the issue of academic freedom. According to Judge Wilkinson,

> [t]o begin and end the public concern inquiry with the signature on plaintiffs' paychecks or the serial number on their computers [i.e., because they are government employees using government equipment] would be to permit all manner of content- and viewpoint-based restrictions on speech and research conducted in our universities. . . .
>
> By embracing the Commonwealth's view that all work-related speech by public employees is beyond public concern, the majority sanctions state legislative interference in public universities without limit. The majority's position would plainly allow the prohibition of speech on matters of public concern. . . .
>
> By upholding this statute on the first step [i.e., the "public concern" analysis] . . . the majority surrenders this balance [between the citizen's and the state's interests] to a world of absolutes.[57]

The *Urofsky* case, until it is modified or overturned, clearly confers extensive authority on North Carolina government employers to regulate employees' use of government computers. It also appears to reject the notion that state-employed educators have much, if any, constitutionally protected academic freedom. Although the case involved university professors, it is safe to say that school boards have the right to

53. When the employer asserts that the adverse action taken against the employee was motivated by reasons other than the employee's speech, the employee must show that the speech *was* a motivating factor and the employer must show that it would have taken the same action regardless of the speech.

54. 216 F.3d 401 (4th Cir. 2000), *cert. denied*, 531 U.S. 1070 (2001).

55. The case's significance and complexity are indicated by the fact that it generated five separate opinions: one majority, three concurring (i.e., agreeing in the result but elaborating or offering different reasons), and one dissenting.

56. *Urofsky*, 216 F.3d at 409.

57. *Id.* at 429–30, 434.

control school employees' use of school-owned electronic resources, even for academic purposes.

Cases in other jurisdictions also indicate support for government control of employee computer use. For example, a three-judge New York appellate panel upheld a state agency's right to terminate an employee's e-mail privilege for sending union-related material. The employee had received several warnings about violating a state policy prohibiting electronic transfers not related to the workplace.[58] In another case, a University of Wisconsin graduate assistant sued the university after her supervisor requested that she remove a quotation from her e-mail signature.[59] (Every message sent from the student's account automatically included the statement: "The truth shall set you free, but first it will piss you off!"). The student claimed the school violated her First Amendment rights by requesting the removal of the statement and by retaliating against her by terminating her after she refused to remove the quotation.

The court ruled that the student's e-mail quotation did not amount to a matter of public concern because it was primarily personal in nature. The court recognized that many statements are both public and personal but found that a statement fails the "public concern" prong of the analysis if the private element predominates. The court held that although her statement did address a matter of public concern, her repeated use of the quotation in every e-mail made it more of a personal statement.

Practical Considerations

School officials should consider the following points when deciding employee cyberspeech issues:

- Determine what policies, if any, are necessary to limit employee use of school-provided computers. Any policy should be based on sound managerial and educational reasons, not a desire to limit the expression of unpopular opinions.
- Provide a procedural mechanism by which employees may challenge or question a particular restriction and through which exceptions to normal policies may be granted when potential free speech rights are at stake.
- Proceed cautiously when restricting speech or disciplining employees for expressing their opinion, via school computers, on a matter of public concern. In most cases, legal counsel should be sought before making a decision.

58. www.law.com, April 29, 2002.

59. Pichelmann v. Madsen, 31 Fed. Appx. 322 (7th Cir. 2002).

Defamation

Defamation—an attack upon the reputation of another—is a complex area of law made more so by its cyberdimensions. Because neither face-to-face nor voice contact is required in electronic communication, some of the natural inhibitors in regular communications are missing when parties communicate by e-mail.

> [E-mail] is remarkably quick and easy to use. Comments can be typed in haste and sent at the press of a button. . . . As a result, email correspondence is often in substance more like spoken conversation than written interaction for habitual users—hasty, ungrammatical and rash—and tends to lead parties to say things they would not only not normally commit to writing, let alone widely published writing, but would in fact often also not say in face to face interaction with the other party. . . . All this means that those sending email are dangerously prone to making remarks that turn out to be legally actionable.[60]

Generally, to prove an allegation of defamation, a plaintiff must demonstrate three things: (1) that a false statement was made about him or her; (2) that the false statement was communicated to at least one other person; and (3) that the false statement caused injury to the plaintiff's reputation. (In some instances, injury is presumed to occur.)

The case law on the liability of school systems and officials for electronic defamation is sparse. In the following sections we consider several categories of potential defamation actions.[61]

60. Lilian Edwards, "Defamation and the Internet: Name Calling in Cyberspace," in *Law and the Internet: Regulating Cyberspace*, ed. Lilian Edwards and Charlotte Waelde (Oxford, 1997).

61. One question that arises is, What court can you sue in for a claim of electronic defamation? In December 2002, the Fourth Circuit Court of Appeals denied a Virginia prison warden the opportunity to sue several Connecticut newspapers for articles published in that state on the Internet. The articles contained allegedly defamatory information about the warden, implying that he was a racist and ran a Virginia prison that mistreated prisoners transferred from Connecticut. Relying on prior precedent, the court had to determine whether (1) the defendants "directed" electronic activity into Virginia; (2) they intended to engage in business within the state; and (3) the action posed a recognizable legal claim within the state. The court ruled that Virginia did not have jurisdiction over the matter because the defendants did not "manifest an intent to aim their website or posted articles at a Virginia audience." The mere fact, said the court, that articles are posted on the Internet and may be read by viewers from another state does not automatically confer jurisdiction on that state. Young v. New Haven Advocate, 315 F.3d 256; 2002 (4th Cir. 2002), *cert. denied*, 123 S. Ct. 2092 (2003).

A similar situation arose in North Dakota after an expelled university student allegedly defamed a professor on her personal Internet Web site. The former student, who later lived and ran the Web site in Minnesota, claimed that the North Dakota court lacked jurisdiction over her, but the North Dakota Supreme Court disagreed. That court ruled that the former student "directly targeted North Dakota with her Web site, specifically [the professor]," by including multiple news articles and links to the university and its staff. Wagner v. Miskin, 660 N.W.2d 593 (2003), available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=nd&vol=20020200&invol=1 (last visited January 20, 2004).

Defamation *by* School Officials and Staff

The ease and speed with which employees can send electronic communications containing sensitive and potentially defamatory information increases the risk of defamation suits. School officials may rely on one of the traditional defenses to defamation charges (e.g., the communication was true, or was not published, or was subject to a special legal privilege). They may find, however, that the unique characteristics of electronic media increase the chances that these defenses will fail. The qualified privilege defense, for example, generally applies to disclosure of false and defamatory employee information when (1) the person making and the person receiving the communication (e.g., former and prospective supervisors) both have a legitimate interest or duty associated with the subject of the communication; (2) the matter communicated is relevant (e.g., it relates to job performance); and (3) the communication is made without malice (i.e., the communicator did not know, and could not reasonably know, that the statement was false).[62] An e-mail message accidentally sent by a supervisor to the wrong recipient or containing information inappropriate for the recipient to view could nullify the qualified privilege.

These dangers require e-mail users to avoid communicating sensitive information electronically or to use special caution when doing so; for example,

- taking extra care when addressing electronic communications and/or attaching documents,
- employing password-protection methods to safeguard sensitive information,
- being reasonably sure of the security of electronic communication lines,
- periodically reminding employees of the dangers of and precautions required when sending sensitive information.

Such precautions not only reduce the risk of errant communications but also provide evidence to a court that a defendant has made reasonable efforts to safeguard information.

Defamation *of* School Officials and Staff

Occasionally, lawsuits arise after students or others post Web pages or send e-mail messages that criticize school officials.[63] One recent North Carolina case involved a Wilkes County principal and teacher who sued the Rutherford Institute (a religious-freedom advocacy organization) after the institute published an on-line article falsely accusing the principal and teacher of denying a student her First Amendment rights.[64] (The student later retracted the accusation, and the institute published a retraction.) The district court ruled in favor of the institute, noting that the plaintiffs did not establish that it had acted with "actual malice" (a required First Amendment element of proof in such cases). The Fourth Circuit Court of Appeals found that the district court had erred by addressing the constitutional issue of "actual malice" before determining whether the Institute had actually defamed the educators under North Carolina state law. The appeals court sent the case back to the district court for reconsideration.

On remand, the magistrate judge eventually ruled for the defendants. Following instructions from the Fourth Circuit, the magistrate first considered whether the speech in question was defamatory under North Carolina law. Specifically, the judge considered two categories of libel: (1) libel *per quod*, which requires proof not only of negligence on the part of the publisher of the statement but also of actual damages suffered; and (2) libel *per se*, which requires no proof of negligence or injury—because injury is presumed—if the publication alleges conduct of an egregious nature (e.g., committing an infamous crime or immoral act, having an infectious disease, or discrediting a person in his or her profession).

The magistrate first ruled that the teacher and principal failed to prove libel *per quod* because they failed to show that the defendants acted negligently or that the plaintiffs suffered actual damages. The magistrate went on, however, to rule that the article and news releases were libelous *per se* because they impugned the plaintiffs' integrity as professionals.

> [P]ublic school educators occupy professions that are of extraordinary interest not only to students and their families, but also to the general public as well. [I]t is also obvious that allegations that a public school educator had denied a student of her constitutional rights to freedom of speech and religious expression would "tend . . . to impeach [that teacher or principal] in that person's trade or profession."

Having ruled that the defendants' press releases and Internet postings did not constitute libel *per quod* but did constitute libel *per se*, the judge had one more task: to determine whether the plaintiffs were public officials against whom the defendants acted with "actual malice." In the 1964 landmark case of *New York Times Co. v. Sullivan*, the U.S. Supreme

62. North Carolina essentially codified this common law defense several years ago when it enacted Gen. Stat. § 1-539.12 (hereinafter G.S.).

63. For instance, Internet faculty rating systems are starting to increase on U.S. college campuses. Factrac, a student-run system at Williams College, began operating on the Internet in April 2002. It quickly reported close to a thousand postings. Most of Williams's 270 professors united against the system, but the college refused to delete the site from its campus computer network. However, Williams worked out an arrangement to limit access to the site to the 2,000 students registered at the college. Paul Eng, "Making the Grade," ABCNews.com (last visited February 25, 2004).

64. Hugger v. Rutherford Institute, 2003 U.S. App. LEXIS 8391 (4th Cir. May 2, 2003; Unpublished Opinion).

Court ruled that the First and Fourteenth Amendments to the U.S. Constitution prohibit a public official from recovering damages on a state defamation claim unless the official proves that the defendant acted with "actual malice," (i.e., published defamatory material knowingly or with reckless disregard of its truth).[65]

Prior to *Hugger v. Rutherford*, no North Carolina court had determined whether teachers or principals are public officials. (Being considered a public official has various legal ramifications, including heightened evidentiary requirements for defamation.) This case is significant because the magistrate determined that the teacher and the principal *are* public officials. In this instance, the facts alleged by the plaintiffs failed to show that the defendants acted with actual malice. On the contrary, the court noted, the institute published prompt and extensive retractions when it discovered the false nature of the allegations and made efforts, initially and repeatedly, to verify the student's allegations. The magistrate therefore dismissed the plaintiffs' defamation claims.

Another case worth noting involved an alleged defamation not of individual educators but of a whole school system. In *Port Arthur Independent School District v. Klein & Associates Political Relations*, a Texas appellate court ruled that a school system, as a government entity, was not entitled to bring a libel suit against an Internet publisher that allegedly communicated defamatory information about a prom conducted at one of the system's schools.[66]

Liability of School Systems as Internet Service Providers

Under some circumstances, a school system that offers Internet and e-mail services to students and staff may be considered an Internet service provider (ISP). Consequently, it may face lawsuits when users of the service disseminate defamatory communications over the system's network—just as a book publisher can be sued when an author writes defamatory passages in a book it publishes.

In most cases, however, ISPs are protected from liability for defamatory communications created by individual users and transmitted through the ISP's network. The relevant subsections of Section 230 of the federal Communications Decency Act (CDA) of 1996 read as follows:

> (c)(1) No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. . . .
>
> (f)(2) The term "interactive computer service" means an information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet and such systems operated or services offered by libraries or *educational institutions* [italics added].[67]

Public school systems offering network computer access, Internet access, or e-mail services thus appear to be immune from liability under these provisions. But even though court cases testing these provisions have mostly been brought against private ISPs like America Online (AOL), Prodigy, and CompuServ, the rulings in these cases are relevant to school system providers.

One of the early cases arose in the Fourth Circuit Court of Appeals (which has jurisdiction over North Carolina) in *Zeran v. America Online, Inc.*[68] That case involved an AOL electronic bulletin board service that contained several messages from an unknown poster advertising "Naughty Oklahoma T-Shirts." The posting listed the telephone number of Ken Zeran (who ran a home-based business) and described the shirts, which allegedly featured offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Zeran, who had neither created such shirts nor had any intention of selling them, received numerous angry calls and physical threats after an Oklahoma radio station encouraged listeners to call his home number to register complaints.

When Zeran notified AOL of the false posting, AOL refused to post a retraction but eventually cut off services to the individual responsible for the messages. Zeran subsequently sued AOL for defamation, claiming that once he notified AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material. The court ruled in favor of AOL under Section 230 of the CDA. According to the court,

> [b]y its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—[are] barred.[69]

65. 376 U.S. 254 (1964).
66. 70 S.W.3d 349 (Tx. App. 2002).
67. 47 U.S.C. § 230.
68. 129 F.3d 327, 329 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998).
69. *Id.* at 330–31.

The court noted that Congress had passed Section 230: to avoid the impracticalities of forcing ISPs to monitor the voluminous communications transmitted over their servers, to promote open communications, and to encourage self-policing activities by ISPs (the reasoning being that ISPs are unlikely to monitor communications if doing so establishes an act of control that increases their risk of liability).[70] According to the *Zeran* court, the plaintiff's notice of the defamatory communication to AOL and the latter's refusal to issue a retraction or monitor future messages were not evidence that it had sufficient control over communications to make it liable for their defamatory content.

It appears that other courts have generally followed *Zeran*.[71] In 2003 the Ninth Circuit Court of Appeals ruled against an Asheville, North Carolina, plaintiff who claimed that the defendant, the manager of an international lost artwork Web site based in the Netherlands, had defamed her when he distributed an e-mail message received from the plaintiff's handyman.[72] The handyman's e-mail asserted that the plaintiff had boasted to him that she was the granddaughter of World War II German General Heinrich Himmler and that she had inherited her large personal art collection from him. The handyman sent the e-mail in the belief that the plaintiff wrongfully possessed the artwork in question. The defendant had then posted the e-mail in an internationally distributed listserv message. When the plaintiff eventually found out about the posting, she filed suit in California, claiming injury to her personal and professional reputation. (Because of the publication, she, as an attorney, became the subject of an investigation by the North Carolina State Bar.) In his defense, the defendant claimed immunity under § 230(c) of the CDA, and the court concurred, noting the difference between cyberspace and regular defamation law.

> There is no reason inherent in the technological features of cyberspace why First Amendment and defamation law should apply differently in cyberspace than in the brick and mortar world. Congress, however, has chosen for policy reasons [e.g., to promote cyber-commerce and free speech] to immunize from liability for defamatory or obscene speech "providers and users of interactive computer services" when the defamatory or obscene material is "provided" by someone else.[73]

It appears that school systems, too, to the extent that they act as ISPs, are protected, especially if they don't exercise substantial editorial control. School officials should therefore determine in advance

1. whether and under what conditions to grant e-mail services and Internet access to staff and students, and
2. the extent to which they will monitor and control such access.

Several considerations apply to these decisions. First, because school systems appear to have broad protection as ISPs under Section 230, it is not imprudent for schools to offer Internet and e-mail service to students and employees. Second, if a school system contracts with other persons or entities to provide Web management or content, it may avoid liability for defamatory distribution caused by the contractor as long as it does not exercise editorial control over the contractor's work. Third, schools and school systems should adopt measures to minimize defamation liability, in particular an acceptable-use policy (AUP) that instructs users on the risks and responsibilities of using school computers.

School officials also should keep in mind that it is against state law to send (or allow 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."[74] Notifying users of these criminal prohibitions may also help schools decrease the risk of defamation suits.

---

70. "If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. . . . Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech." *Id.* at 333, citing Auvil v. CBS 60 Minutes, 800 F. Supp. 928, 931 (E.D. Wash. 1992) (recognizing that it is unrealistic for network affiliates to "monitor incoming transmissions and exercise on-the-spot discretionary calls") and Philadelphia Newspapers, Inc. v. Hepps , 475 U.S. 767, 777 (1986).

71. See Carafano v. Metrosplash.com, Inc., No. 02-55658, 2003 U.S. App. LEXIS 16548 (9th Cir. 2003) (noting "the consensus developing across other courts of appeals that § 230(c) provides broad immunity for publishing content provided primarily by third parties") and citing Green v. America Online, 318 F.3d 465, 470–71 (3d Cir. 2003) (upholding immunity for the transmission of defamatory messages and a program designed to disrupt the recipient's computer) and Ben Ezra, Weinstein, & Co. v. America Online Inc., 206 F.3d 980, 985–86 (10th Cir. 2000) (upholding immunity for the on-line provision of stock information even though AOL communicated frequently with the stock-quote providers and had occasionally deleted stock symbols and other information from its database in an effort to correct errors).

72. Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003).

73. *Id.* at 1020.

74. G.S. 14-196.3.

Conclusion

Technology, which offers numerous educational and administrative benefits, also creates new challenges for school officials. The case law and other rules to provide some clarity about the legal boundaries that govern electronic technologies are only now beginning to take shape. Administrators need to tread carefully when making decisions about expanding or restricting technology use in schools—taking their time, considering the implications of their decisions, and, when feasible, involving an attorney. It is important to carefully review the initial technology decisions, monitor technology use, and periodically reassess the school system's technology practices and policies. Finally, school officials need to stay tuned while judges, legislators, and rule makers continue to determine how laws, new and old, should be applied to the expanding use of technology in our schools. ■