ence, and to test what students know of these, typically leaves little time or energy for something like teaching cyberethics. In the amalgam of connected 21st century “global villages,” regardless of how you answer the question: “what is the aim of education?” we have to ask: is teaching cyberethics not worth it? And, if so, do we have the courage to do so?

**The Case for Cyberethics**

In the twenty-first century, computing and the Internet have become ubiquitous, at least in the developed world. The Internet is everywhere, and, as Moor explained, “computing technology is not running away from us as much as moving in with us. Computer sprawl, like urban sprawl, moves inexorably on many fronts unsupervised” (Moor, 2000, p. 35). The problem with “unsupervised” technology is that as computing creeps into all aspects of life, the ethical implications are often unexamined. Just acquiring, installing, operating, and dealing with technology consumes so much time and energy that, often, little is left for examining its impact and its relationship to right and wrong. The demands of the marketplace are so great, so competitive, that as Moor says, “When a new computer technology is ready for market, nobody asks about its ethical implications. They may come later if at all.”

However, the time to acquire ethical practices and habits in computing comes early. Both Berkowitz (2000) and Yamano (2004) put it at ages 9–12, or roughly between grades 4 and 7 in schools. Certainly by age nine, most children in the developed world have had experience with computing both at home and increasingly in school, at the library, and with various games and toys. By age nine children are beginning to form habits of turning to computers and the Internet for information, to communicate with their friends, and to play. Habits are, of course, crucial to ethical behavior; as Moor reminds us, “Our character in turn arises out of our habits. One has character of courage, temperance, honesty, and so on because one has built these dispositions as habits over time. Early training is imperative for Aristotle. As he says,
‘it makes no small difference, then, whether we form habits of one kind or another from our very youth, it makes a very great difference, or rather all the difference’” (Moor, 2000, p. 39).

Yamano (2004) studied how prepared fourth and fifth grade teachers feel in teaching their students about cyberethics. She found that while most teachers, as adults, have a strong sense of personal ethics and are able to practice that in cyberspace, they have a great deal of difficulty transferring that moral understanding into teaching cyberethics to their students. Yamano found that most teachers are working at learning to use computing and the Internet in support of achieving learning objectives. When it comes to cyberethics, with the exception of copyright and plagiarism, concepts that transfer more easily from the paper world to the digital world, they have had neither the time nor the training to extend their educational work with computing to ethical behavior. As Patty Yamano found in her research, “teachers tended toward a very general understanding of responsible use of technology and teaching students about responsible use in very general ways and were not comfortable teaching specific concepts about cyberethics . . . such as filtering and social implications” (p. 106). Just as significant, she found that even though a minority of teachers were teaching about cyberethics, those teachers were doing so in direct instruction rather than through activities and discussion, the kinds of interactive process so necessary in developing judgment.

Nancy Willard (2002) reminds us of what is at stake in the case for cyberethics. She recounts the wisdom of the Confucian analects where, “the Master said, If the people be led by laws, and uniformity sought to be given them by punishments, they will try to avoid the punishment, but have no sense of shame . . . If they be led by virtue, and uniformity sought to be given them by the rules of propriety, they will have the sense of shame, and moreover will become good” (the Analects, n.d.). Of course, while the prospect or reality of shame can be a powerful motivator, the desire to do what is right out of respect for oneself and others is likely more powerful, at least in the long run. Respect for oneself and others is a virtuous goal of much
parenting but its development through feeling and thinking about how unethical, malicious behaviors may be hurtful relates so much to virtues of respect and responsibility in schools that it is easy to see its importance both in and out of school. However, when developing these traits in cyberspace, we must overcome the ways in which the virtual world is typically intangible, invisible, and easily delayed or ignored. In cyberspace, the ways in which unethical behavior inflicts hurt or pain is typically abstract and removed from the hurt look of an embarrassed classmate suffering from a mean rumor overheard in the hallway. We must help young people in building the cognitive or thinking part of understanding that harmful acts in cyberspace actually do hurt people.

**School-Oriented Cyberethics and Character Education**

Patty Yamano has a formula for cyberethics and Patty, an elementary school teacher in the Los Angeles Unified School District for 30 years, knows the value of an easy to remember formula. Her formula is not, however, a formula like those favored in math class that yield a correct calculation, or like a recipe where if you follow it precisely, the result is a consistent product. Patty’s formula has to do with human concerns, with pesky values and ethics and morals on the Internet where the signs that trigger well-known moral responses are not always so easy to read. This is where Patty’s formula is useful yet it is a formula about which many people appear to know very little and although some are running hard to improve the condition of their knowledge, we still have a long way to go. Her formula, and cyberethics in general, speaks to what we and our children are about as human beings and it is something about which, compared to the vast oceans of data we have on every kid’s ability to supply answers on standardized tests, we appear to know very little. Patty’s formula is concerned with ethical behavior on the Internet, or, more comprehensively, in cyberspace. Moreover, it would seem to require very little imagination to think of
the consequences of our teachers and our children understanding her formulation, well or poorly.

When you think about it, needing a formula to remember what ethics are when computing is itself revealing. Cyberethics are just new enough and vague enough that many people still are not sure exactly what they are. Patty’s formula, based on the work of ethicist Marvin Berkowitz (2000), could help and it goes like this: P3 H2 C. In this formula, P3 is not three of the same element but three different ethical concerns beginning with the letter P: privacy, personal identity, and plagiarism. H2 stands for two additional concerns: hacking and hate speech, and C stands for the one of the most ubiquitous concerns: copyright. In many ways, this formula captures an appropriately manageable set of cyberethics in schools and provides a toehold for knowing what to address (Yamano, 2004). Privacy, for example, is extremely limited in schools for, with all the inappropriate material on the Internet, and with all the concerns about youngsters being distracted by entertainment and appearances, not to mention overexposing themselves on the Internet, there is little if any Internet privacy in schools. Evidence of this limitation comes from the Massachusetts’ department of education report citing that “The law requires schools to certify that they have an Internet safety policy and that they are using filtering to block visual images that are obscene, child pornographic, or harmful to minors. In 2005, more than 99 percent of schools had such filters” (Massachusetts Department of Education, 2006).

The issue of privacy on the Internet in schools today is set in the turbulent context of a historic struggle to define the issue in society. This makes privacy of primary importance in considering Patty’s formula.

**Privacy**

Privacy in cyberspace is one of the most complicated issues facing all of us today. When searching for “privacy on the internet” in June 2006,
Google returned over two billion hits. A look at the Yahoo News page on online privacy returned five “news stories,” six “feature articles,” six “opinion and editorial” articles, six “related Web sites” and each category had links to more sites (Yahoo News, June 16, 2006). Much of the cause of this interest is the effort of multitudes to determine just what privacy is in cyberspace.

The Center for Democracy and Technology (CDT) describes three areas as constituting normal expectations of privacy: anonymity in public spaces, fairness and control of personal information, and reasonable expectations of confidentiality of personal records and communication (Berman and Mulligan, 1999). It is probably fair to say that average, naïve Internet users assume or had assumed a certain degree of these privacies on the Internet. However, the nature of digital Internet technology makes recording and monitoring of a user’s information relatively easy. Thus, it is easy to violate average user’s reasonable expectation of privacy on the Internet. Recording a user’s “click stream” or “mouse droppings” is currently so easy and so unprotected by the law that the issue is not if a person’s actions on the Internet are observed and recorded. They typically are. The issue is what is legal and ethical to record and what it is legal and ethical to do with that information once recorded.

Privacy in electronic-based communication is still being settled as a legal issue, especially in light of the “war on terror” being waged by the G.W. Bush administration. In their efforts to fight terrorism and crime, the U.S. federal government is working hard to have access to all of the public’s email and telephone conversations. Ho, Richman, and Lewis (2006) report that the federal government has asked for, and seeks to require, all Web Internet Service Providers (ISPs) such as Microsoft, Google, AOL, Comcast, and so on to collect and preserve all records of their customers’ use of the Internet for up to two years. This, along with recent revelations that the National Security Administration (NSA) is collecting information on all telephone calls from the telephone companies suddenly makes nearly all electronic based communications subject to investigation by anyone who can get a subpoena.
As threatening to reasonable expectations of privacy as government or other civil court access to private communication seems, it probably pales in comparison to the way commercial organizations collect and now correlate everything one does on the Internet. These companies use this information to develop a “profile” of every user in order to target advertising to each person’s particular interests to increase the probability that the advertising will lead to sales. If you read about sports on the Internet, for example, and buy a pair of sneakers online, the next time you log into your favorite online sports news source, a national, sport’s supply company ad pops into your field of dreams.

The CDT describes online profiling as akin to walking into a mall “where every store, unbeknownst to you, placed a sign on your back. The signs tell every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet” (Berman and Mulligan, 1999, p. 4). Without legal protection, the Internet is already a place where anonymity is an illusion unless one takes specific steps to try to ensure it by purchasing software that hides the IP address and information of the user; for example, “Anonymizer” offers software that “protects your personal email address and your identity disposable, anonymous email addresses” (http://www.anonymizer.com/default.html).

As early as 2001, Schwartau observed that, “privacy is going away, bit by bit” (Schwartau, 2001). It did not take long, for in 2006, privacy is virtually nonexistent. Yet, evidence abounds that many people agree that privacy is a basic human right. Article 12 of the Universal Declaration of Human Rights, adopted by the General Assembly on December 10, 1948 states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks” (United Nations, n.d.). The Fourth Amendment to the U.S. Constitution states: “The right of the people to be secure in
their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized” (Findlaw, n.d.). Further, no discussion of privacy, no matter how limited, is complete without mention of Justice Louis D. Brandeis’ view that privacy is “The right to be left alone” (Langheinrich, 2002; Brandeis and Warren, 1890).

Despite privacy guides, guarantees, and precedents, it is, on the Internet at least, somewhat of an illusion. This essay began with a description of how schools are able to monitor “every click you make.” When online at home or outside of school, people easily feel they are alone because they may be alone in their physical space. Online, however, monitoring and collection of data, although unnoticeable, is becoming a de facto standard and this is an issue or phenomenon about which young people, but especially teenagers, need to know. People have a right to know who is watching them and why, even if the watchers are their parents and protectors.

The need for privacy is not the same as the need for security in online purchases. Encryption algorithms, for example, more or less guarantee the security of credit card numbers at least during transmission over the Internet, but privacy or being anonymous or unobserved on the Internet is another matter. While one can think when you go online that you are poking your head out unnoticed into cyberspace like a prairie dog on the plains of the American West, Internet companies, the government, marketing organizations, thieves, and ordinary individuals with the right software can surreptitiously collect data on your every move on the Internet. While encryption of credit card and other personal information addresses security concerns in financial transactions, it may be best to assume there is otherwise no such thing as privacy in cyberspace. It is just that the observers are usually invisible. This larger societal context makes the issue of privacy in schools appear small in comparison but nevertheless, schools must address what they do and what they communicate to their users about
the limitations on privacy in using the Internet when logged into the schools’ Internet service.

Schools want to allow and support the use of the Internet in support of teaching and learning. The content of teaching and learning is public, and therefore, it is safe to assume that there is no privacy on the Internet in schools. However, that does not mean that a student or teacher could not have a private email account. It does mean that schools can monitor email accounts to ensure students and staff are using them in support of reasonable educational activities. Students also have a right to have their work and records kept private so only the owner, their parents, and appropriate teachers and educational staff have access and that no work would be made public without permission. Hence, despite the need of schools to limit and monitor students access to the Internet to ensure that the content is appropriate, students still have some need for privacy.

One of the most important ethical issues related to privacy in using computer networks in schools is the privacy of passwords. It is unethical to steal or copy someone else’s password and then use it to see their private information. Thus, schooling in the need to protect one’s own and respect others’ passwords is an issue in schools and with children who are of an age where sharing personal information with friends is often of paramount importance in building relationships. These competing forces make the situation ripe for abuse but also ripe for learning how violating the ethical necessity of protecting one’s own and respecting others’ passwords can cause harm to people. This situation is useful for demonstrating that ethical violations in cyberspace have consequences, real consequences.

To help children conceptualize what is appropriate for them to share online, Willard (2002) recommends using the “front page test.” Would you want, she asks, the information you share to appear on the front page of your local newspaper or on your local TV news program? Children need help in developing the ability to think before they click.

Willard also sounds the alarm on online profiling. Despite COPPA, the Children’s Online Privacy Protection Act (http://www
which became effective on April 21, 2000 and which limits the information that a Web site or online service can collect on children under 13, companies have ways to tease information out of young and old alike. The purpose of Internet surveys, polls, registrations, and all manner of enticing rewards that pop up on the screen of Internet users is typically to collect information about users. It is important for students and teachers to understand that this information can be stored indefinitely in databases where it can be later accessed and potentially correlated with other sources of data about the user. It may be helpful for children, she suggests, to use the “check inside test” before providing any personal information online. In this test, the user should ask him or herself “do I want my information to be kept in a computer database” over which I will have no control “for years in the future?” (Willard, 2002, p. 28). This is a reflective, think before you click “gut check” discouraged by our relentlessly fast-paced society, but its value may be more evident in this context than some others in the real world. Although it is often hard for young people to imagine that their interests will change in years to come, the current lack of enforcement of existing legal protections of online information as well as the lack of it for children 13 and over, means that data is routinely collected for the determined investigator to harvest, no matter their motivations.

The way in which commercial, political, even government organizations can harvest and use information stored in databases extends the notion of privacy in the Googling age. Notions of privacy can now extend to include the ideas that an Internet user should have the “freedom from being contacted without permission” and that it is unethical to “infringe on other’s privacy—go where you’re not supposed to go” (Yamano, 2006). In this context the need to educate both teachers and students about their presumed expectations of, and the contradictory reality of, privacy on the Internet is essential education for safety as well as for becoming informed citizens in the Googling age.

The multiple dimensions of privacy demonstrate the complexity that while the reality of Internet use out-of-school may be undermining,