Who Determines What Our Children See, Read, Do, or Learn on the Internet?

Sondlo Leonard Mhlaba
Wentworth Institute of Technology

Follow this and additional works at: http://scholarworks.umb.edu/trotter_review

Part of the Communication Technology and New Media Commons, Educational Administration and Supervision Commons, Science and Technology Policy Commons, and the Science and Technology Studies Commons

Recommended Citation
Available at: http://scholarworks.umb.edu/trotter_review/vol9/iss2/4

This Article is brought to you for free and open access by the William Monroe Trotter Institute at ScholarWorks at UMass Boston. It has been accepted for inclusion in Trotter Review by an authorized administrator of ScholarWorks at UMass Boston. For more information, please contact library.uasc@umb.edu.
Who Determines What Our Children See, Read, Do, or Learn on the Internet?

by Sondlo Leonard Mhlaba

Monitoring the Internet

The issue of appropriate use of the Internet at home and in schools is being hotly debated right now in, and outside, the Internet. In March 1995 Marlene Goss wrote a letter to the discussion list of the Consortium for School Networking (CoSNdisc@list.cred.net) appealing to educational policymakers to focus on access and equity when dealing with Internet in schools, instead of focusing on restricting such access. She found it remarkable how many hours were being spent “deciding student use when only 3% of the classroom teachers, professional adults, have use of the Internet.” Her point was not so much that students should have unlimited access, but that teachers and other educators should not be denied access under the guise of protecting children. Educators, she argued, “make intelligent decisions about what we expose our students to, daily.”

In response, this writer partially agrees with Goss, but worries that monitoring access to the Internet is the kind of challenge that is not familiar to parents and teachers. Most parents and teachers are accustomed to the challenges of monitoring what children watch on television. Monitoring computer use, however, is very different. Once a youngster is logged on the information superhighway, he or she has the capacity to roam the world. Unlike television where parents either know the schedule or can see what the youngster is watching, computers tend to be in places where a child can explore the world unobserved. To some extent this is not a big problem in schools because the computer room is usually supervised. Even with good supervision in schools however, there is the problem that the Internet traveler sits right in front of the tube, with the ability to obscure what he or she is reading, sending, or viewing.

Jack Crawford of the K12Net Council of Coordinators raised additional, vexing, constitutional and legal questions which attend control of Internet access:

If a school takes an active role in attempting to control what students have access to on the Internet (via school-based equipment), and a student finds some “bad stuff” anyways, can the school be held liable for failing to “protect” the student? What if the school is an Internet provider equipped to provide access to kids from their home computers. Is the school liable for what the kids can get into while logged on at home?

These are questions which parents, educators, courts, and government need to wrestle with, and resolve sooner than later. At this point no one is sure how to proceed. Recent court decisions concerning alleged misuses on the information superhighway have had the appearance of discouraging close supervision of bulletin boards at a time when parents and educators are looking for more supervision, not less. In Cubby v. CompuServe, 776F. Supp. 135 (S. D. N.Y. 1991), the court found in favor of CompuServe specifically because the company argued that it was merely a system operator and could not be expected to keep tabs on all communications on its bulletin board. In this case Cubby, Inc., as plaintiff, had accused CompuServe of defaming it through its bulletin board. More recently in May 1995, the New York Superior Court, Nassau County, appears to have continued the line of reasoning applied in Cubby v. CompuServe by ruling against Prodigy in Stratton Oakmont v. Prodigy, principally because Prodigy has promoted itself as a keen monitor of its bulletin boards. Stratton Oakmont, Inc., an investment firm, had brought suit against Prodigy essentially for imputing its integrity through a bulletin board that Prodigy owns.

In Congress several pieces of legislation are in the works, which attempt to regulate the content of electronic communications. Among these is a version of Senator Exon’s “Communications Decency Act of 1995,” which is now part of S. 652, the “Telecommunications Competition and Deregulation Act of 1995.” Several versions of Senator Exon’s draft bill are now appearing in many state legislatures; and have the potential of being over-restrictive and probably unconstitutional. These attempts at regulation of electronic discourse attest to the difficulty of the task. If parents and educators can find the answers for our limited area of interest, perhaps the rest of society may benefit, in due course. But parents and educators cannot make a contribution until they get themselves as
informed as possible about the information revolution that
is upon us and, in particular, their children. Below is a
background summary on the Internet which may help us
appreciate its power and the complexity of its control.

The Evolution of the Internet
The Internet evolved from the Advanced Research
Project of the Department of Defense (DOD). DOD
funded several universities and corporations to create a
digital communication network (ARPANET) that was
separate from the telephone system. The primary purpose
of this ARPANET was to ensure that DOD
communication links survived a nuclear attack or other
violent eruptions that might result from an earthquake.
ARPANET became operational in 1969 using four
computers. By the 1970s, it had grown to over 100
computers. When DOD reduced its support for
ARPANET in the 1980s, the National Science Foundation
(NSF) stepped in and supported a restructured ARPANET
which was not tied to defense and was available to
universities without restriction. The new network was also
made available to commercial concerns for a fee. This
expanded system became the “backbone” of an entire
collection of networks known as the Internet. The Internet
has since become a global web linking over 100 countries
and nearly 3 million computers.

What we now commonly call cyberspace is an
agglomeration of networks, including commercial on-line
services such as America On-Line and CompuServe,
Computer Bulletin Boards (BBSs) large and small, and
networks of networks such as the Internet. As the
technology has advanced, it has become feasible to
transmit data, voice and pictures across the planet at the
blink of an eye. Under current rules, what you send or
receive is up to you or any other person who can access
your address. You can exchange essays on the origin of
the universe or converse about the joys of birdwatching.
But you can also send or receive something which is
objectionable to the general public.

Although there are organizational structures and codes
of conduct among user groups, more often than not, the
system is seen by friend and foe alike as essentially
ungoverned and, at worst, anarchic and fertile ground for
criminal activity. The problem within this structure or
structurelessness has been brought home to many recently
by reports of actual as well as potential crimes. Below is a
sample of such reports:

• A commercial access provider, Panix Public Access, had
to shut down its system for three days when it
discovered a “trojan horse” program in one of its
computers in October 1993. By the time the foreign
program was discovered, it was feared, it might have
already allowed “a secret group of computer hackers to
run wild through hundreds of government, university,
and commercial computers, purloining information right
and left and wreaking who knows what damage…”

• The Department of Justice proposes to strengthen the
Computer Fraud and Abuse Act of 1986 to enable it to
crack down on such crimes as, “credit history report
thefts, sales of stolen passwords and illegal use of
telecommunications services.”

• CERT, the Carnegie Mellon University-based
Computer Emergency Response Team, had received
close to 1,500 calls for help in fighting computer crime
in 1993. That figure represented a 75% increase in such
calls in one year.

• In Bucland Hills Mall in Manchester, CT an automatic
teller machine was programmed by crooks to steal
ATM card numbers for unauthorized entry into other
people’s cash accounts. Fifty thousand dollars was
stolen before the crime ring was broken. Susan Trausche
who reported on this crime called it a “classic white-
collar crime. No dynamite, no guns, no masks, no
cops.”

• Mr. Alden J. Baker, Jr., allegedly, enticed young boys
to engage in sexual acts in his Medford home. It was
also speculated that Mr. Baker photographed the young
boys as they performed for his enjoyment, and
transferred the images into a computer bulletin board
for transmission, locally and internationally, to fee-
paying subscribers.

Efforts to Protect Our Children
We need to accept the fact that the Internet is here to
stay and to understand its significance to 21st century
civilization. Thus, we must ensure that our young people
at home and in schools are exposed to this technology,
“The risk of not acting,” asserts Beth Gold-Bernstein, “is
being left behind. How can we adequately prepare our
students for their world, if we do not provide them with
the primary interface to the Information Age?”

Indeed, several schools and school systems around
the country are joining the global information infrastructure
(GII). In Lexington, Massachusetts, the school system is
exploring a system-wide connection to the electronic
highway and is already researching appropriate use
policies (AUPs) for the Internet. The State of Iowa has
probably the most sophisticated, statewide system in place
today. Completed in 1993, the approximately 3,000-mile
network carries voice, data, full-motion, two-way,
interative video, high definition television, high
resolution graphics, and computer-aided design to some
125 locations in the state. The system is being used for
“expanding the state’s educational opportunities; sharing
limited and/or costly resources; . . . providing specialized
classes to schools that could not afford them otherwise;
connecting student teachers in the field with their
professors…”

Perhaps the most exciting development in the GII is the
Bay Area Multimedia Technology Alliance (BAMTA), a
newly formed public-private research alliance formed
with help from a $5 million grant from the National
Aeronautics and Space Administration (NASA). BAMTA
will explore barriers to the distribution of multimedia over
a network. Some of the technical barriers which they hope
to overcome relate to “transmission protocols, image
compression, copyrights, collaborative authoring tools
and indexing, storing, searching, browsing and retrieval of
multimedia content." Three initial pilot projects have been identified: 1) aerospace; 2) health care; and, 3) education.

Access and equity are, indeed, major concerns of people working in the field of educational telecommunications.

Efforts are also underway to address issues of access and equity. As the Telecommunications Reform Bill goes through Congress this year, advocates will be watching to ensure that the legislation addresses the issue of equity and access. In a draft letter to the Senate Commerce Committee which is presently working on the Bill, Mr. Bill Wright of the Consortium for School Networking (CoSN) wrote:

Telecommunications technologies will open new doors of educational opportunities for our children. Access to the GII is critical to ensuring that our children can succeed in an increasingly technological world marketplace. However, for schools to have meaningful access to telecommunications and information services, access must be universal and affordable. While opening up the telecommunications marketplace to increased competition stands to increase affordability, our long-term educational interests demand including that goal specifically in legislation.

Other equity and access efforts are directly aimed at minority communities which are at higher risk of being left behind. Among organizations in the forefront of such efforts is Quality Education For Minorities (QEM) Network of Washington, D. C. One of QEM’s innovative projects is to electronically link low-income, public housing residents with selected, predominantly minority institutions. “Technology offers the best chance,” says QEM’s President Shirley McBay, “for leveling the academic playing field for children and youth from low-income families.” To ensure access and equity, these advocates will push for, among other things, a technology that is both affordable and user-friendly. Access and equity are, indeed, major concerns of people working in the field of educational telecommunications.

A Proposal

Because the electronic highway knows no state or national boundaries, efforts to control what our children see, read, learn or do on the Internet must be joined at several levels and involve both technological and administrative strategies. These levels must include:

1. International efforts carried out under the auspices of such agencies as the United Nations Telecommunications Union (ITU), the World Trade Organization (WTO), and Interpol, to name a few. Through such agencies, broad parameters must be negotiated to meet the diverse cultures, laws, statutes, and educational philosophies. In addition, agreements should be sought to standardize relevant hardware and software, interconnecting protocols, law enforcement interventions, as well as cryptographic guidelines.

2. National strategies that can be appropriately linked to the above. Because of its leadership in telecommunications technology, the U. S. has had a bit of a head start in crafting national legislation to meet the challenges of the GII. In its intellectual property protections, for instance, the U. S. has already ensured coincidence with the related international statute: the Berne Convention. Where the U. S. is ahead of the international community, the U. S. laws can serve as models. Our laws already cover privacy of electronic communications; illegal access to and disclosure of stored communications; transportation of obscene matter for sale or distribution; child pornography; and so forth. As part of the Telecommunications Reform Bill currently before the Senate Commerce Committee (as of late April, 1995), the U. S. should include a section which 1) encourages effective utilization of educational telecommunications in schools and homes; 2) holds schools harmless in the event of system abuses beyond the schools’ control; and, 3) assures swift and harsh punishment for those who blatantly subject children and youth to inappropriate electronic contacts. Finally, the new legislation should 4) require that all electronic mail include the address of the sender which can easily be traced to a legal name.

To be effective however, such legislation should include funding to help school systems purchase hardware and software and, in particular, to provide training for teachers. Survey results from the National Center for Educational Statistics indicate that only 3% of our nation’s classrooms have access to the Internet or use information services for instructional purposes. A recent report of the U. S. Office of Technology Assessment (OTA) entitled, “Teachers and Technology: Making the Connection,” states that even though $2.13 billion were spent on public K-12 instructional technology in 1993, a substantial number of teachers reported little or no use of computers for instruction. The OTA report suggests that lack of teacher training on the use of this resource may be part of the problem. Increased material resources, teacher training and pedagogical changes in schools would help create a climate where the telecommunications technology would be an accepted and normal part of the educational enterprise and, thereby, less susceptible to abuse.

3. This progressive narrowing of regulatory and administrative focus should continue to the state level; and broad appropriate use policies (AUPs) and laws should be a part of statewide educational governance.

4. If the above levels have achieved their goals, then the local level will be left with adequate latitude to
maximize the value of educational telecommunications without the burden of liability or of unduly policing students. The bulk of the local school’s work would be to effectively articulate the community’s values and standards of interpersonal etiquette which apply in verbal as well as electronic communication.

5. At home, parents should encourage moderation in the use of computers, especially for real-time communication, games, and virtual socializing. Some of these activities can be addictive and youngsters can lose a sense of reality. But parents should also realize that the computer network can be a source of exposure to a universe of information and education which was inconceivable only a few years ago. For example, when youngsters do their school assignments, the tasks can become take-off points for in-depth studies of class topics way beyond the teachers’ fondest hopes.

**Conclusion**

Before parents and educators worry themselves silly about the dangers of access to the electronic highway, they must remember the violence, sex, and crime which characterize television programs 24 hours a day. Even the most “kid-oriented” programs on Nickelodeon are unable to resist the sleaze that sells adult movies and books. Yet we continue to keep one, two, or three television sets in our homes, often with questionable monitoring of what our children watch. The Internet and educational CD-ROM programs now available to families through the computer may yet wean our children from the television and close the gap between school and home.

What should our children see, read, learn or do on the Internet? And who should decide? Perhaps the answer to both questions is that they will see, learn, read, and do what we, as parents and educators, help them to see, learn, read and do. If we do not help them, or do not take an interest in what they do, an interested partner may appear in cyberspace and take our youngsters to worlds we do not know.

---

**Notes**

1. Marlene Goss, “A Sincere Letter.” Available from Discussion List of the Consortium for Educational Networking (CoSN); e-mail address: Info@cosn.org.
4. Jack Crawford, “Editorial Liability.” Available from Discussion List of the Consortium for Educational Networking (CoSN); e-mail address: Info@cosn.org.
5. Richard Grayson, “On-Line Defamation.” Available from Discussion List of the Consortium for Educational Networking (CoSN); e-mail address: Info@cosn.org.
12. See “Application Profile—Expanding State Services,” In Iowa Government Circles, Communication is a Piece of Cake, a publication of the State of Iowa, July 1994.
14. From a letter drafted by Bill Wright, administrator of the CoSN Discussion List, which was distributed to national organizations representing local school boards, teachers, administrators, and education technology advocates, to use as a starting point in a campaign to convince the U.S. Congress to include universal and affordable access to telecommunications bill currently being negotiated.
17. Ibid.

Sondlo Leonard Mhlaba is the director of the Academic Resource Center and assistant professor of Applied Mathematics and Sciences at Wentworth Institute of Technology.