Access, Control and Growth of Internet: Discussion (A Case Study)

Internet in Schools

Over the past decade, the number of schools with Internet access has grown exponentially, and the number of children going online from school has followed suit. In 1999, the National Center for Education Statistics reported, 95 percent of public schools were connected to the Internet, and, more importantly, 63 percent of public school classrooms had an Internet connection.

Now, some 14 million children access the Internet from school, a figure that is expected to grow to more than 30 million by 2003 as schools continue to build their networks. By that year, it is anticipated that more students will access the Internet from their classrooms than the number who will access it from home

Concern

The Internet truly is like “a vast library including millions of readily available and indexed publications,” containing content “as diverse as human thought,” as the U.S. Supreme Court described it in a 1997 decision. **But just as in any city frequented by millions of people, there are neighborhoods on the Internet that are inappropriate for children to visit alone and strangers they would be better off not meeting.**

Throughout the past decade, policy makers, industry advocates, parents and teachers have tried to address these concerns.

Meanwhile, a number of initiatives have been launched that were designed to help educate adults about how to protect children when they go online. These projects and tools have included “Child Safety on the Information Highway,” published by the National Center for Missing and Exploited Children and the Interactive Services Association in 1994, Project OPEN (the Online Public Education Network), organized by the ISA and the National Consumers’ League in 1996, the Direct Marketing Association’s “Get CyberSavvy” program in 1997, the American Library Association’s “KidsConnect,” as well as “America Links Up” and “Get Net Wise,” both sponsored by a broad coalition of industry and non-profit groups. All of these initiatives have made useful contributions that educators and parents can continue to use to teach children “the rules of the road” when they go online.

What Is the Source of the Concern?

In the early 1990s, as the number of subscribers to proprietary online systems grew, transforming those communities from the moral equivalent of small towns to large cities or even states, children began to meet people in online chat rooms who would engage in inappropriate conversations or encourage them to divulge information about themselves. Then as proprietary systems such as America Online, Prodigy and CompuServe connected their users to the Internet, and more households accessed the Internet directly through Internet service providers, online users began moving easily to the wide open, unregulated spaces of the World Wide Web.

As the number of Internet users grew, the Internet changed as well. No longer was it a small, tightly knit community of academics, researchers and scientists, where all users generally supported an unwritten code of good behavior. With the advent of the World Wide Web, anyone could open up a store or publish a magazine. Some experts argue that the Web is expanding so fast that it is virtually impossible to track every site that could be objectionable.

A related debate rages over what percentage of Web sites would truly be considered objectionable. Some advocates argue that sites that would be considered harmful to minors represent only a very small proportion of the Web. What is of greater concern, they say, is that perfectly benign and possibly very useful information could be blocked when software is used to screen inappropriate material.

For others, however, the actual extent to which adult-oriented materials are available on the Internet is irrelevant. Because it is possible for children to access such materials without the traditional-world protections of brown-paper wrappers or adult-bookstore doorways, they argue, the existence of any pornographic material is sufficient cause for concern. Those who support government-mandated content controls tend to argue that any amount of inappropriate content is too much, when children are concerned

Pornography is not the only issue involved. Many adults are concerned about Web sites that are created by hate groups or devoted to topics such as bomb-making and weaponry, gambling or alcohol and smoking. Although pornography on the Internet has captured the greatest attention on the part of policy-makers, it is not the only area of potential concern for parents and educators.

How Big Is the Problem?

Data

According to some estimates, the World Wide Web now includes 1.5 billion pages and new Web sites spring up at the rate of 4,400 per day. Cyveillance, a company that monitors the Internet for business clients, estimated in July 2000 that the Web included 2.1 billion pages, with 7 million new pages created each day. Many Web sites are abandoned, or rarely updated, but continue to persist on servers around the world, where anyone in the world can still access them.

In 1995, a study conducted by Marty Rimm, an engineering student at Carnegie-Mellon University, asserted that 83.5 percent of the pictures transmitted through UseNet newsgroups were sexually explicit. His findings were given additional credence when Time magazine featured the study in a cover story headlined “On a Screen Near You: Cyberporn!” Subsequently, the study was discredited and Time backed down from its story. But average Americans, not to mention members of Congress, were left with the perception that pornography could be easily found on the Internet, just a mouse click away. Advocacy groups from the conservative end of the political spectrum contend that there are between 72,000 and 100,000 sexually explicit sites on the Internet and that 85 percent of the 3,900 new sites that are created each day, sell commercial pornography.

Yet another study, by researchers at the University of Pennsylvania’s Annenberg School for Communications, reviewed a random selection of Web pages turned up by a search engine and found that no more than 3.6 percent had “highly objectionable” material, only 2.4 percent had “provocative sexual content” and only 0.7 percent had “notable violent content.”

The World Wide Web, however, is not the only source of concern. Children can receive e-mail messages with pornographic file attachments and e-mail from UsetNet groups, which communicate through an older Internet protocol, can contain postings from users that would be considered inappropriate. Of special concern, too, are Internet chat rooms and so-called Instant Messaging, where children can communicate online in real-time with adult strangers who may not have their best interests at heart.

How Concerned Are Parents?

If children apparently *are* accessing materials that could be considered inappropriate, how concerned are their parents?

America Online officials say that about two-thirds of their user households with children make use of the online service’s parental controls features. However, the National Center for Missing and Exploited Children found in its survey that only about one-third of the families used filtering or blocking software, including software offered by an Internet service provider. A survey conducted by the Annenberg Public Policy Center found a similar percentage of families that used filters, despite the fact that 76 percent of those parents said they were concerned that their children might view sexually explicit images on the Internet. (Interestingly, a greater percentage of parents (82 percent) were worried about what their children might encounter online when their families did not have internet access

Another recent survey of the general public found that while 71 percent believed the Internet could enhance their educational level and 86 percent said it would help their children learn more, there were still concerns about the kind of content that could be accessed. Seventy-six percent said they thought that “inappropriate content” could be a barrier to Internet adoption and 61 percent were worried about the potential impact of “dangerous ideas.”

The conclusion that some researchers have drawn from these surveys is that parents believe that the Internet can be an unsafe place, but are not particularly worried that their own children are getting into trouble. The children, it appears, are not always talking about what they are finding when they go online.

The Legal and Regulatory Backdrop

Despite the development of new software products, rating systems, and industry-supported online safety campaigns, Congress continued to regard the situation with alarm. In 1996, it passed the Communications Decency Act, which prohibited the posting of materials on the World Wide Web that would be considered “indecent” or “patently offensive.” The legislation did not address the dissemination of child pornography or child stalking on the

Internet, which, it was generally agreed, would be prohibited by existing laws. However, in 1997, in a decision known as *Reno v. ACLU* (or commonly as *Reno I*), the Supreme Court unanimously ruled that the measure was much too broad and amounted to an unconstitutional restriction on free speech.

Congress tried again the next year, passing the Child Online Protection Act, which made it a crime to communicate through the Web information that would be considered “harmful to minors” unless access was restricted through the use of a credit card. Violators could be subject to criminal penalties of up to $50,000 a day. In February 1999, a federal district judge blocked enforcement of the act, a decision that was supported by the U.S. Court of Appeals for the 3rd Circuit in a June 2000 decision known as *ACLU v. Reno III.* Once again, the judge ruled that the measure amounted to an impermissible restriction on free speech. Critics of the law noted that the legislation would have had no bearing on Web sites hosted on servers outside the United States, or on other kinds of Internet communications such as e-mail. In May 2001, as expected, the Supreme Court agreed to review the decision.

In December 2000, Congress passed the Children’s Internet Protection Act and Neighborhood Internet Protection Act (commonly referred to as CIPA or “the CHIP Act”) as amendments to the fiscal 2001 appropriations bill for the U.S. Department of Education. This measure will require schools that accept federal E-rate discounts to purchase Internet access or internal connections or that use funding under Title III of the Elementary and Secondary Education Act to purchase Internet access or computers that access the Internet to adopt an “Internet safety policy” and a technology protection measure that blocks or filters content that is obscene, child pornography or “harmful to minors.”

An Opportunity for Learning

Some educators argue that instead of relying on filtering technology to block inappropriate content, schools should focus on teaching students how to evaluate Internet content and to form their own judgments on what is inappropriate. By relying on filtering software, they argue, schools may miss an opportunity to prepare students for what they are likely to encounter in an unfiltered environment, such as through their home computer, a friend’s computer, a university network when they go off to college or a company’s computer when they enter the workforce. Further, the rapidly evolving nature of the Internet virtually ensures that no filtering technology can be 100 percent perfect. Thus, even when a school uses a particular solution, children should be taught how to respond if they still manage to access something that it is inappropriate for them.

Further, the dangers that children can encounter online are not limited to off-color Web sites. Unsupervised chat rooms and so-called Instant Messaging functionality can enable adults to contact children, sometimes posing as children or offering enticements for further real-world contact. When schools begin accessing the Internet, with or without content controls, they should make sure that children are armed with the same kind of safety advice that parents and teachers would normally provide about the dangers of the traditional world: “don’t talk with strangers and don’t give out information about yourself.”

Whether or not a school district decides to use a technological approach to manage content, it would be well advised to promote “information literacy,” that is, teaching children how to find good sources of information online and how to evaluate online information, as well as how to protect themselves when they go online.

What the Future Holds

As with all aspects of technology, the tools and solutions for managing Internet content are continuing to evolve. But so too are the methods that unscrupulous Internet users and merchants can use to lure children to places and materials that could be considered inappropriate for minors.

So far, most of the focus of Internet filtering products—and government policy makers—has been on controlling access to obscene or pornographic Web sites. But that is only part of the content management problem. Children can receive e-mail with pornographic attachments. In addition, functions like chat and Instant Messaging, which children enjoy and which can promote interactivity, can also expose them to potentially dangerous adults, posing as children or sympathetic mentors, if the network is not restricted to children. Many products are beginning to address these problems and providing parents and educators with tools to limit children’s access to them—or to provide greater assurances that the “friends” they meet in chat rooms are indeed children. Unsolicited e-mail, or “spam” as it is commonly called, continues to be a problem for adults as well as children, not to mention system operators.

Another source of concern is about a practice known as “mouse-trapping,” in which an Internet user requests a certain site, but is routed to another one, often featuring adult-oriented content. What makes this practice particularly onerous is that the user finds that the only way he can leave the site is to shut down his browser. The

COPA Commission, for one, has recommended that government regulators try to fight this practice through existing consumer-protection laws aimed at deceptive advertising.

Questions to Ask When Deciding Whether to Manage Content

✓**How will students use the Internet?**

The planning process for every school technology initiative should address this question. Is it anticipated that students will be using the Internet unsupervised, as a research tool? Or will teachers be managing their experiences more closely? How many computers are in classrooms, labs and media centers and how will that impact the ability of school staff to closely monitor how students are using the Internet? Answering these questions will help determine whether students' Internet access should be supervised and whether staff will be in a position to do it on their own.

✓**Do you want students to be able to direct their own learning or is it more important for teachers to retain control of what goes on in the classroom?**

To what extent does your school or school district foster a classroom culture in which students are independent learners? Or are you more comfortable with a more structured, more formal classroom model? How your school or school district answers this question will provide guidance on how comfortable you will be with giving students unrestricted access to the Internet.

✓**Should different standards be applied, based on the age of the student?**

Your district may decide that different approaches are appropriate, depending, say, on whether a student is in high school or elementary school. If so, you will want to make sure that your proposed solution will give you that flexibility. You may decide to adopt content controls only in certain schools, or you may decide to choose a product that will let you set different levels of restriction for different age groups or classes.

✓**Should school employees be subject to the same rules as students, to their own set of rules or to no rules?**

Are you concerned about how your employees will use the school district's online resources? If so, what kind of rules or limits do you want to impose? Should staff members be required to follow the same rules that students do, or is it more appropriate to adopt a separate policy for adults? Should you distinguish between the kind of online activities they pursue during school hours and those that they pursue outside of school hours?

✓**Would you prefer to simply monitor how students and employees use the Internet, rather than blocking their access to sites?** Would this approach raise any privacy concerns? Will your staff have time to monitor these logs and respond to potential abuses?

✓**Are there other issues that you want to address at the same time?**

Some content management solutions address other concerns about the Internet or network operations. These include protecting a school network against hackers or viruses, protecting the privacy of students, and restricting children's exposure to advertising messages. If so, you may wish to evaluate whether a certain approach will provide a cost-effective solution to more than one problem.

✓**How will school officials respond if students are found to be accessing inappropriate material?**

This issue should be addressed in your Acceptable Use Policy. Students should know how they are expected to respond if they access a clearly inappropriate site, whether or not it was intentional.

✓**What strategies will your school district use to teach "information literacy?"**

No matter what approach a school district takes, it should ensure that its students understand the "rules of the road" when they go online and how to evaluate the content that they find there. These lessons can be imparted either as part of regular online classwork, or as special activities that must be completed before a student can go online.

Questions to Consider When Evaluating Content Management Products

✓**Who should make the decision on what kind of sites are blocked or accessed?**

If school personnel will make the decision on which sites students will be allowed to access, will they have enough time to devote to that task? How frequently will they be able to update their lists? Who will be responsible for updating the list of approved sites? Will that give students access to a wide enough variety of sites?

If a third party will make the decision on which sites will be blocked or accessed**,** do you understand the criteria it uses to evaluate Web sites? Does the organization or company have any particular bias? How easy will it be for school personnel to override those decisions if they disagree with them? How frequently does the organization or company update its lists of sites, and how easily is that update accomplished?

✓**What kinds of content are you concerned about?**

Are you primarily concerned about children's access to pornography and obscenity, or are you concerned about their access to materials on topics such as weapons, hate groups and alternative lifestyles?

✓**What has the experience been with the solution you propose to use?**

To what extent are children able to access inappropriate sites, either directly or through search engines and other links? If a product appears to be effective in blocking problem sites, does it go too far in also blocking sites that would be considered benign or needed by a class studying a sensitive topic? A team of staff members may want to test proposed solutions to see what kind of results they turn up. Research papers and testimony compiled by the COPA Commission provides information about the methods that have been used by other researchers to test the effectiveness of blocking software.

✓**How are users notified when they try to access a blocked site?**

Some products provide a clear notice when a site has been blocked. Some allow this message to be tailored to the network's needs. Some products block in a more invisible way. Is it important for your Internet users, both students and staff, to know if they have tried to access sites that were blocked? Or would you prefer that this information be withheld?

✓**Does the proposed solution address other forms of content besides just Web sites?**

Does it provide tools for controlling such things as e-mail, access to chat rooms, and Instant Messaging? Is it important for your solution to include that kind of functionality?

✓**How easy would it be for a child to hack into and disable a particular filtering solution?**

Generally, tools are more difficult to disable when installed on a server, whether it belongs to a school, an Internet service provider or a filtering company, than they are when installed on a desktop computer.

✓**Does the proposed solution incorporate advertising messages? Will third parties be able to collect information about how your students are accessing the Internet?**

Some products incorporate these features, sometimes in exchange for reduced fees, or no fees at all for the product or service. School officials should understand whether advertising or marketing messages are incorporated into a product and what information, if any, will be gathered about users, either individually or in aggregate. Sites that gather information about children are now subject to the Children's Online Privacy Protection Act and the role schools are expected to play in the administration of this law is still under discussion.

✓**If your students speak many different languages, does your proposed solution control access to sites written in languages other than English?**

Some children learn to subvert content controls by making their requests in a foreign language. Further, if a child's native language is something other than English, will he receive the same level of protection that a child typing in Web site names in English would?

✓**How will the proposed solution serve your district in the future?**

Will the solution still work as the number of Internet-accessible computers grows? How will that change the price? What future enhancements are on the drawing boards? If your district plans to let children access the Internet through other kinds of devices, how will you extend the controls to those products?