Cyber-Democracy or Cyber-Hegemony? Exploring the Political and Economic Structures of the Internet as an Alternative Source of Information

Julie Frechette

Abstract

Although government regulation of the Internet has been decried as undercutting free speech, the control of Internet content through capitalist gateways—namely, profit-driven software companies—has gone largely uncriticized. The author argues that this discursive trend manufactures consent through a hegemonic force neglecting to confront the invasion of online advertising or marketing strategies directed at children. This study suggests that "inappropriate content" (that is, nudity, pornography, obscenities) constitutes a cultural currency through which concerns and responses to the Internet have been articulated within the mainstream. By examining the rhetorical and financial investments of the telecommunications business sector, the author contends that the rhetorical elements creating "cyber-safety" concerns within the mainstream attempt to reach the consent of parents and educators by asking them to see some Internet content as value laden (sexuality, trigger words, or adult content), while disguising the interests and authority of profitable computer software and hardware industries (advertising and marketing). Although most online "safety measures" neglect to confront the emerging invasion of advertising/marketing directed at children and youth, the author argues that media literacy in cyberspace demands such scrutiny. Unlike measures to block or filter online information, students need an empowerment approach that will enable them to analyze, evaluate, and judge the information they receive.

According to figures provided by the U.S. Census Bureau (2001), more than half of school-age children (6 to 17 years) had access to computers

Julie Frechette, Associate Professor of Communications Studies, Worcester State College, 486 Chandler St., Worcester, MA 01602
LIBRARY TRENDS, Vol. 53, No. 4, Spring 2005 ("The Commercialized Web: Challenges for Libraries and Democracy," edited by Bettina Fabos), pp. 555–575

both in school and at home in the year 2000 (57 percent). With some 17 million children using the Internet in some capacity, including email, the Web, chat rooms, and instant messaging (Silver and Garland, 2004, p. 158), the Census Bureau estimates that 21 percent use the Internet to perform school-related tasks, such as research for assignments or taking courses online.

While these statistics underscore the growth and popularity of the Internet, particularly in schools and educational institutions, concerns have grown about the "safety" of using computer-mediated communication technology. Since the Internet became a mass medium in 1995, parents and schools have approached online content with reservation. As such, politicians, educators, child advocacy groups, and, most importantly, the computer industry, have been vocal advocates for patrolling the Internet and censoring certain kinds of illicit or objectionable content. Beginning in the late 1990s, Federal Trade Commission member Christine Varney summarized the emerging concerns about online safety:

> All of us agree that children's online safety concerns are real and pressing and that we must support the involvement of parents raising children in this new, digital age. We understand that we must all work together—industry, law enforcement, educators, advocates—if American families are to realize the potential of this new medium for enriching the lives of our children and fostering their future success. (Rubin and Lamb, 1997)

Starting in 1997, an Internet/Online Summit was held in Washington, D.C., to enhance the safety and benefits of cyberspace for children and families. Key political figures, such as former vice president Al Gore and former attorney general Janet Reno, joined parents, as well as politicians, law enforcement officials, and educational administrators, to launch a national public education campaign, "America Links Up: An Internet Teach-In," designed to help Americans understand how to guide kids online (Rubin & Lamb, 1997).

On October 21, 1998, former president Bill Clinton signed into law the "Children's Online Privacy Protection Act" (COPPA). This measure was enacted by Congress on April 21, 2000, to "prohibit unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally identifiable information from and about children on the Internet" under the age of thirteen (Grossman, 2000). Along this trajectory, Congress passed the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NCIPA) in December 2000, which required schools and libraries that receive federal money for Internet connections to adopt Internet safety policies in 2001. The proposed safety measures include usage agreements for proper student use of this medium, audit-tracking devices to supervise student Internet perusal, and software

filtration devices designed to block inappropriate sites in schools (Trotter, 2001).

In 2002 the Bush administration proposed a "National Strategy to Secure Cyber Space," offering security recommendations for U.S. citizens, businesses, and organizations using computers (Carlson, 2002). Since then the Federal Trade Commission has offered testimony before special committees and the House of Representatives about online pornography through a series of "law enforcement actions against fraud artists whose deceptive or unfair practices involve exposing consumers, including children, to unwanted pornography on the Internet" (Federal Trade Commission, 2004, p. 1).

In addition to these federal initiatives, many states have measures designed to protect children from online predators. In Texas, Attorney General Greg Abbott added more investigators to the Texas Internet Bureau to keep kids safe from those who use online means to prey on children. As Assistant Attorney General Sparks explained, "The Attorney General wants the public to know that he's tasking people with patrolling the Internet and trying to make it safe for kids; the down side is that more and more children on a daily basis are getting online and on the Internet and as every additional child gets on, that's one more potential target" (quoted in Ochoa, 2003).

Likewise, educators have expressed concerns about online information overload. According to one school administrator, accessing the Internet in schools is less predictable: "If you used to bring your class to the school library, you pretty much had a sense of what was available for the children to research; now you have no idea . . . they are going to hit sites that are appropriate and sites that are inappropriate" (quoted in Shyles, 2003, p. 176).

Despite a commitment to online "security" in schools, libraries, and homes from so many constituents, few recommendations have materialized into solid strategies or funding initiatives. Almost all of the proposed solutions and policies ignore the more relevant question of how private computer companies, Internet service providers, corporations, and governments stand to gain financially and politically by deciding what kind of information will be "censored" and what kind will be promoted. In fact, it could be argued that the Internet content "crisis" dominating public policy and mainstream media coverage has produced a cultural climate ripe for the commercial exploitation of parents and educators. In this article I argue that such a discursive trend manufactures consent through a hegemonic force that overlooks the invasion of advertising or marketing strategies targeted at young people online. By examining the rhetorical and financial investments of the telecommunications business sector, I contend that the mainstream articulation of "Internet safety" invites parents and educators to regard *some* Internet content as value-laden (sexuality, obscene language),

while disguising the interests and authority of profit-minded commercial enterprise (advertising and marketing).

What is more, the democratic potential of the Internet as a means to accessing alternative information and perspectives otherwise absent from the mainstream media continues to be threatened by the consolidation of increasingly powerful global media giants, such as Time Warner and Microsoft, which have much to gain from controlling the content Internet users access at home or at school. Consequently, an examination of the political and economic forces on the Internet is necessary for librarians and educators interested in understanding the benefits and limits of the Internet as a means of alternative communication.

Exploring the Means to Filtering Online Content

Parental Guidance

As a result of this discourse, a number of solutions have been advanced to ward off illicit content appearing on the computer screens of young Internet users, beginning with parental guidance. CyberTipLine grew out of the 1997 Internet/Online Summit and is currently in operation today. Run by the U.S. government and the National Center for Missing and Exploited Children, parents can notify authorities of incidents of online child pornography and child predation. Another derivative of the summit's "America Links Up" project is the industry-sponsored "GetNetWise" Web site, which was launched in 1999. The "user empowerment" service, which involves a coalition of numerous Internet industry partners and advocacy organizations,[1] offers parental advice, including information about filters to block sexually explicit material, as well as a variety of tools to help parents and caregivers monitor a child's online activities and find browsers for kid-friendly sites. As one sponsor, AT&T, notes in its promotional material, "Our involvement with GetNetWise reflects our commitment to help users have the best possible online experience" (GetNetWise, 2004).

A more well-known parental guidance initiative, passed in April 2000, was the Children's Online Privacy Protection Act (COPPA). In accordance with COPPA, the Federal Bureau of Investigation offers "A Parent's Guide to Internet Safety," which advises parents to "utilize parental controls provided by your service provider and/or blocking software" and "Monitor your child's access to all types of live electronic communications (chat rooms, instant messages, Internet Relay Chat, etc.), and monitor your child's e-mail" (Federal Bureau of Investigation, 2004).

Other parental guidance measures have been created to address online advertising and marketing as well as issues of privacy. Parent advocacy groups, such as Commercial Alert, Consumer Action, the Center for Media Education, and Computer Professionals for Social Responsibility, have taken up the cause of parents concerned about online marketing measures

targeted at children. For example, Commercial Alert has made requests to the Federal Communications Commission and the Federal Trade Commission to require disclosure of embedded advertising in a variety of media and has created a "Parent's Bill of Rights" seeking to empower parents in the face of an aggressive commercial culture (Commercial Alert, 2003).

Proof-of-Age/Shielding Systems

In addition to parental guidance, many online providers and Webmasters have adopted proof-of-age/shielding systems that use credit card access as another means of content filtering. While COPPA sought to protect children thirteen and under, those located in the fourteen to eighteen year range were not covered by legislation. Providing proof of age before being allowed to access the content of a desired online site emerged as a means to address this gap. This system works in the same way that fraud-screening technology works: merchants collect user information at their Web sites for instant age or identity verification. Once online users submit their name, zip code, date of birth, and age, they are checked through an international electronic database of government-issued identifications. This allows site providers or merchants to determine the consumer's identity within seconds. Sometimes additional measures, such as online name signature, are required so that user signatures are bound to a public record.

Proprietary Environments

Another reaction to the discourse of online safety has been the advocacy of proprietary environments, where content is screened by editors into specific categories. For example, the leading Internet service provider, America Online (AOL), provides a blocking service that allows users (ostensibly parents) to limit a child's selected screen name to either a "Kids Only" area, which is recommended for children under twelve, or to a preteen/teen environment, with restricted use of chat rooms or newsgroups. According to the site, "Kids Only" is a collection of educational resources and entertainment areas as well as a preselected collection of child-oriented Internet sites, with AOL staff monitoring of message boards and chat rooms. AOL also promotes the company's "Parental Phone Line" for instructions and advice on choosing and maintaining the settings of this product (the premise here is that the settings are likely to be tampered with by savvy teens and preteens).

In addition to "Kids Only," AOL has aggressively marketed its AOL@School service, which had been adopted by more than 14,000 schools by 2004 (Williams, 2003). AOL@School offers six online learning portals for grades K–5, middle school, and high school so that students can access Web sites that have been preselected by educators as content and age appropriate. The software needed to access the portals comes with AOL's "parental controls" designed to "help ensure a safe, secure, age-appropriate experience" that can include school-controlled email, chat, and instant

messaging (AOL, 2004). The popularity of "child safe" proprietary environments has not waned as Web browsers and popular search engines have created their own directories in an attempt to create safe havens for (and develop customer loyalty from) younger online users. Yahooligans' "Web Guide for Kids" is a collection of predominantly commercial links to online games, music, TV, science, news, jokes, "cool pages," arts and entertainment, and sports. Like most commercial proprietary environments, Yahooligans is riddled with advertisements and synergistic ties to commercial media products.

Internet Ratings Systems

For those seeking additional regulatory measures, Internet rating systems offer another approach. Unlike the rating system for television content that is uniformly and centrally organized by the television industry, Internet ratings are not assigned consistently by a centralized group of online content providers. The goal is the same, however: industry self-regulation over government regulation. According to ratings system advocates, many of whom work in the software and computer industry, Internet ratings are designed to make it "safe" for schools and parents to let their children access nonpornographic material without government directives. According to Paul Resnick, chairman of the World Wide Web Consortium group at the MIT Laboratory for Computer Science, which includes AT&T Laboratories and Microsoft, the Platform for Internet Content Selection (PICS) was originally created to allow parents, teachers, and librarians to review questionable materials that they would not want their children to come across on the Internet (Resnick, 1997).

Resnick explains, "prior to PICS there was no standard format for labels, so companies that wished to provide access control had to both develop the software and provide the labels. PICS provides a common format for labels, so that any PICS-compliant selection software can process any PICS-compliant label" (Resnick, 1997, p. 107). Yet unlike uniform rating labels,

> a single site or document may have many labels, provided by different organizations. Consumers choose their selection software and their label sources (called *rating services*) independently. This separation allows both markets to flourish: companies that prefer to remain value-neutral can offer selection software without providing any labels; values-oriented organizations, without writing software, can create rating services that provide labels. (Resnick, 1997, p. 107)

One of the leading Internet rating systems that uses PICS is SafeSurf, a group that offers ratings along with other tools to help parents and "net citizens" filter online information. One means to achieving its goal is to encourage online content providers to fill out a questionnaire using content descriptors to rate their Web sites. Unlike government- or industry-wide regulatory labeling efforts that may "brand" content, SafeSurf is interested in

maintaining First Amendment rights by offering content providers greater latitude to self-rate their Web material. For example, rather than branding content that includes nudity as pornographic, users can distinguish their inclusion of nudity as scientific, sociocultural, artistic, titillating, graphic, or illegal. Once content providers rate their Web sites or directories, they can download the SafeSurf rated logo of their choice. A SafeSurf staff member verifies the rating and sets up the chosen ratings label. Parents and educators can then use PICS compliant software/browsers to read the settings and to use the ratings to filter content that is not desired. As the SafeSurf group explains, "PICS allows content providers to rate their pages and parents to set passwords and levels for their children. Then, PICS compliant software/browsers will read the settings and use the ratings to filter content that is not desired" (SafeSurf, 2004a).

The Internet Content Rating Association (ICRA) is another international, independent, nonprofit organization that seeks to "empower the public, especially parents, to make informed decisions about electronic media by means of the open and objective labeling of content" (ICRA, 2004). ICRA's dual aims are to "protect children from potentially harmful material and to protect free speech on the internet." Like SafeSurf, Web authors complete an online questionnaire describing the content of their site, upon which ICRA generates a content label using PICS computer coding, which the author adds to his/her site. Parents and Internet users can then set their Internet browser to accept or decline access to Web sites based on the labels and user preferences. PICS is now a standard feature included in Internet software and browsers such as Microsoft Explorer.

Third-Party Rating Systems

While ratings systems are designed to allow content providers to voluntarily label the content they create and distribute, third-party rating systems "enable multiple, independent labeling services to associate additional labels with content created and distributed by others. Services may devise their own labeling systems, and the same content may receive different labels from different services" (ICRA, 2004). In other words, online watchdog groups interested in protecting children from online predators or illicit material can offer their own set of restrictive control tools for material that they deem to be objectionable. One such group is WiredSafety, formerly known as CyberAngels, led by Parry Aftab, an experienced international attorney and author of *The Parent's Guide to Protecting Your Children In Cyberspace* and *A Parent's Guide to the Internet*. Lauded as "one of Internet safety's most influential players," (Hill, 2000), Aftab has emerged as a nonprofit leader who has created coalitions with many governmental and nongovernmental agencies, including the FBI's Innocent Images anti–child pornography and exploitation task force. She was appointed the founding American director of UNESCO's global Child Safeline project and currently heads

WiredSafety, "the largest online safety, education and help group in the world" (WiredSafety, 2004). With more than 9,000 volunteers worldwide, the group is a coalition of various Internet safety groups, such as WiredKids.org, WiredTeens, Teenangels, and CyberMoms and CyberDads, and their affiliate, WiredCops.org, all of whom patrol the Internet for child pornography, child molesters, and cyberstalkers. Additionally, WiredSafety offers a variety of educational and help services for online users. Some of its volunteers access and review family friendly Web sites, filter software products and Internet services, and post their findings on the Web. The group even has a "Cyber911 help line" that offers net users access to help when they need it online. SurfWatch is another online ratings system designed for parental supervision. It too prevents access to Web, gopher, and FTP sites that SurfWatch's team of "net-surfers" have found objectionable. They maintain an updated list of "not-for-children" Web sites that can be subscribed to electronically.

Commercial Filtering Software and Databases

A more intensive effort to censor "inappropriate" online content has come from commercial filtering software companies (often working in conjunction with powerful Internet content providers and third-party ratings systems). Also known as "censorware," these filtering products, which include Net Nanny, CyberPatrol, Cyber Sitter and N2H2, range in cost from $25.99 to $80 and are heavily marketed to parents, educational administrators, and libraries. Designed to be installed on home or school computers or to work with network routers or firewall, cache, or proxy devices, these products claim to offer safety measures for youth using computers for online research and recreation. Essentially, most of these programs work by using a combination of filtering and blocking strategies, such as the blocking of Web sites denoted through keywords and databases and the blocking of individual Web sites by specific URLs.

One of the first filtering programs—and most commercially lucrative—is Net Nanny. According to its promotional Web site, Net Nanny® 5 is "the world's leading parental control software, [and] provides customers with the broadest set of Internet safety tools available today. Our award-winning software gives customers control over what comes into and goes out of their home through their Internet connection, while respecting their personal values and beliefs" (Net Nanny, 2004). Launched in 1998, Net Nanny is a tool allowing parents, teachers, administrators, and librarians to screen incoming and outgoing Internet information, particularly pornographic material. By identifying and blocking various sites and subjects considered inappropriate, the program blocks the Web addresses of known pornographic and illicit sites. Parents can add to the collection of forbidden "code words" used to detect and flag sites. The program works with

all major online providers and in email. It can also prevent children from accessing specific files on a PC's hard drive, floppy drive, or CD-ROM. Like audit-tracking software programs, Net Nanny keeps a record of a child or student's Internet perusal, meaning that parents and teachers can check up on the sites that a child has perused.

With all of these features, it is no surprise that Net Nanny's popularity and financial success has led it to offer additional blocking software such as Net Nanny's Pop-Up Scrubber, which blocks pop-up ads, Net Nanny's Ad-Free, which blocks a range of Internet ads, spyware, and profiling cookies, and Net Nanny's Chat Monitor, which monitors and filters Instant Messaging and other online chat.

Another commercial service, CyberPatrol, works in the same way as Net Nanny by filtering harmful Web sites, newsgroups, and Web-based email. Also commercially successful, CyberPatrol licenses its "CyberLIST" database of site ratings to several additional vendors. Among its ratings categories are violence/profanity, partial nudity, full nudity, sexual acts, gross depictions, intolerance, satanic or cult, drugs and drug culture, militant/extremist, sex education, questionable/illegal and gambling, and alcohol and tobacco. Likewise, Cybersitter blocks sites and subjects deemed unacceptable by Internet users. It offers site lists for automatic blocking and allows parents to have added input in restricting programs, files, and games. According to *PC Magazine,* Cybersitter offers the strongest filtering and monitoring features, blocking content related to violence, hate, sex, and drugs (Munro, 2004). It also allows parents to choose from thirty-two content categories, such as free email sites, file sharing, wrestling, cults, and gambling, for those interested in added blocking categories. As with other similar products, it lets parents filter and monitor their children's activities without their knowledge and can record both sides of Instant Messaging sessions.

Joining in the mix of filtering software providers is N2H2 (acquired by Secure Computing in 2003), a company endorsed by eTesting Labs and the Kaiser Foundation as "the most effective and accurate" filtering program and extensive database of objectionable Internet sites (N2H2, 2004). It offers two product lines: Sentian, which is geared toward helping businesses manage their employee Internet access, and Bess, a popular program and database adopted by many schools and endorsed by the American Library Association to help schools and libraries meet CIPA rules for young Internet users.

With so many companies vying to be the best provider of filtering software, it is not surprising that Microsoft would venture into this area by offering its own industry standard Internet filter aimed at regulating youth-directed online content. As part of its monopoly on the Internet browser software Internet Explorer (which accompanies its Windows platform), Microsoft has also implemented a filtering system that can be configured

to block or log all data transfers, including World Wide Web pages, newsgroups, types of messages within any newsgroup, Internet Relay Chat, or Internet hosts known to have objectionable material for children.

Questioning the Viability of Online "Safety" Initiatives

Although some of these Internet resources and restrictions make sense for certain schools depending upon the age group and grade level of Internet users, there are some problematic areas within each method that should be cause for concern. The main underlying difficulty raised by these "quasi-solutions" is that they narrowly define what is "inappropriate," relegating most objections to issues of nudity, sexuality, trigger words, or adult content. This focus neglects to confront the invasion of advertising or marketing strategies directed at children. In many respects, Internet commercialism seems to be a more serious concern, but one would never guess this considering the ad-strewn and content-compromised "solutions" to appropriate Internet content.

First, although child-directed advertising might not be as blatantly offensive, it certainly fosters "values" that, at present, are not considered objectionable to most governmental, parental, and commercial watchdog groups. Although the first tenet of media literacy explains that *all media are constructions,* the problem with advertising and marketing strategies is that they are so much a part of our social landscape and our everyday life that they appear to be natural. Subsequently, the conceptualization of what is inappropriate for children or students only helps to sustain the interests of a commercial system through the omission of advertising; advertising is omitted and thereby deemed appropriate. Just as parents, educators, and anticommercial groups, such as Commercial Alert, have protested the commercial imperatives of satellite-delivered school programs such as Channel One, a company that offers schools free satellite equipment in exchange for a captive audience of students forced to watch its daily, advertisement-driven programming, and the computer equivalent ZapMe!, which tried to turn "the schools and the compulsory schooling laws into a means of gaining access to a captive audience of children in order to extract market research from them and to advertise to them" (Commercial Alert, 2000), we need to be equally circumspect about the amount of advertising and marketing proliferating on "Kids Only" sites and via kid-safe filtering software (Schiffman, 2000).

Moreover, sustaining an Internet-based market economy whereby consumer software programs and proprietary environments become the antidote to inappropriate material is directly at odds with democratic means of dealing with these issues through public discourse, political action, and critical media literacy skills. Most of the products previously analyzed are produced and distributed by profit-making and publicly traded enterprises,

such as the media conglomerates Time Warner, Microsoft, and Yahoo!. Obviously, it is good business to create and sell blocking software products or to offer third-party rating systems that decide—for parents, educators, and librarians—what is in their (both children/students and the company's) best interest. In a self-fulfilling business transaction, reports of inappropriate content as well as media and political hype about the Internet as an "unsafe environment" lend credence to, or create a functionalist need for, such products. As stated earlier, advertising is overlooked as "inappropriate content" because it is part of everyday consumer culture, unlike pornographic and hate sites, which exist beyond the boundaries of what is deemed "good" for children and teenagers. As Marxist philosopher Antonio Gramsci (1971) has noted, hegemony works within the terrain of everyday life and requires the consent of audiences—or in this case, parents, educators, and librarians. Hence, the commonly employed rhetorical elements that create paranoia about Internet content within the mainstream attempt to reach the consent of parents and educators by inviting them to see some Internet content as value-laden or problematic while camouflaging the interests and authority of a profitable computer software and hardware industry.

Although serious discussion about government regulation goes beyond the purviews of this study, several concerns must be raised regarding commercial software programs. First, the decision to block some sites over others is a very subjective decision. The problem with this kind of regulation is that some groups and individuals might attempt to censor material (under the guise of concerns for "safety") that threaten their own political and/or religious agenda. Dependence upon commercial Internet service providers and related filtering products limits the democratic principle of the free flow of information and puts commercial enterprise at the helm of online navigation, a troubling fact given that corporate culture can often be extremely conservative and self-serving when it comes to making censorship decisions. In one instance, America Online was charged with using filters to block out several Web sites associated with "liberal" political organizations. One of the top stories featured in *Censored 2001* was AOL's liberal blacklist, whereby sites for the Democratic National Committee, Ralph Nader's Green Party, Ross Perot's Reform Party, the Coalition to Stop Gun Violence, and Safer Guns Now were labeled as "not appropriate for children" (Phillips & Project Censored, 2001, p. 111). Ironically, the youth filters did not prevent access to nudity or to conservative groups, including the National Rifle Association. Designed for America Online by the Learning Company, an educational software company owned by Mattel, such filtering programs confirm suspicions about the process of labeling and omitting Web sites according to political and economic interests.

This kind of censorship raises flags about the capabilities of large media conglomerates to limit access to material deemed politically at odds with commercial interests. Inasmuch as Disney was in a position to rebuke the

distribution of *Fahrenheit 9/11,* Michael Moore's political documentary produced through Disney's Miramax film division, large multimedia conglomerates are poised to censor content that is politically or economically damaging to their enterprise.

Second, some of the trigger words used to block Internet sites might be legitimate subjects for research. For example, the often-cited example of an Internet user not being able to access research on breast cancer or sex education (if these words were denoted as trigger words) is indeed troubling. As *PC Magazine* reviewers of Cybersitter 9.0 explain, "Cybersitter errs on the conservative side; by default it may block sites you would deem okay" (Munro, 2004). A telling example of this problem is offered in an article featured in *Electronic School Online.* Author Lars Kongshem writes,

> CYBERsitter yanks offending words from web pages without providing a clue to the reader that the text has been altered. The mangled text that results from this intervention might change the meaning and intent of a sentence dramatically. For example, because "homosexual" is in the list of CYBERsitter's forbidden words, the sentence, "The Catholic church is opposed to all homosexual marriages" appears to the user as, "The Catholic church is opposed to all marriages." (Kongshem, 1998)

Likewise, Karen Schneider, a librarian for the Environmental Protection Agency, has led a filtering software assessment project involving more than thirty librarians around the world. She has found that filters "are not reliable and they're hard to maintain" (cited in Gebeloff, 1999). In one example, recipes using "chicken breast" were blocked due to sensitive word triggers. Rob Gebeloff, author of *Screening Zone: The Trouble with Net Filters and Ratings,* continues to problematize the use of all types of "censorware" programs by pointing out numerous gray areas in judging content. He asks:

> Do you want your kids going to Web sites that discuss birth control? What about AIDS education? Or what about the exploration of Mars? [A recent *New York Times* article pointed out that one filtering program blocked out every Web site with the word "sex" in it, including a site that had the word "marsexploration" in it's title]. So clearly, if you're going to go with filtering, be prepared to make tough calls. (Gebeloff, 1999)

Peacefire—a group critical of filtering software—explains, "We have always felt that filtering software is not only ineffective, but also a violation of the trust between students and staff . . . Unfortunately, most of the censorware companies block anything controversial, not just pornography. I find it very discouraging that this includes information like suicide prevention, safe sex, and gay youth resources" (B. Jenkins, quoted in Kongshem, 1998).

Third, students and computer hackers have already found flaws with such programs and have managed to acquire information from sites that have been blocked. When product evaluators at *Consumer Reports* tested over nine different Web content filters, including AOL's parental controls,

they discovered that, although AOL offered the best protection, as much as 20 percent of easily located Web sites containing sexually explicit content, violently graphic images, or promotion of drugs, tobacco, crime, or bigotry slipped through the filters. In fact, "Net Nanny displayed parts of more than a dozen sites, often with forbidden words expunged but graphic images intact" (ConsumerReports.Org, 2001).

Fourth, there is an inherent conflict of interest when the main advocates challenging the government's attempts to protect children from online predation and pornography are the very same groups that seek to profit directly from a "free marketplace" of online smut. In its June 2004 press release, SafeSurf applauded the Supreme Court for its ruling in the Internet pornography case *Ashcroft v. ACLU* "because the High Court concluded that Internet filtering solutions, such as those originally proposed by SafeSurf over nine years ago, are a better way to proceed than the government restrictions imposed under the Child Online Protection Act" (Jules, 2004). As the chairman of SafeSurf, Ray Soular, exclaimed, "This decision has revealed that the High Court has seen the *wisdom* in protecting the Internet from governmental censorship and in enabling parental discretion through an intelligent filtering and labeling system. Maybe now, Congress will focus more attention on what has become known as the 'Safe Surfing' method of protecting children online" (Jules, 2004, emphasis added). Yet the court's *wisdom* is more the result of intense lobbying than constitutional insight. SafeSurf has been lobbying Congress about the constitutionality of the Child Online Protection Act since its implementation, arguing its case before the Congressional Commission on Child Online Protection (COPA) in July 2000, just a few months after COPA's passage.

Gebeloff addresses this conflict of interest in his critique of net filters and ratings for *Money Talks:*

> I once had a chance to interview Gordon Ross, the fellow who designed Net Nanny. . . . I asked Ross how he, with his background in computer systems, comes up with the list of bad words and unacceptable Web sites that his program blocks. Basically, he told me, it started from a list he put together and then evolved over time to reflect feedback from users. "And we have a disclaimer saying we're not liable for the list." (Gebeloff, 1999)

This leads Gebeloff to deduce the ironic disposition of this practice: "We don't want the government to be our censor, so why should we turn the job over to a computer programmer from British Columbia? The answer, of course, is that we shouldn't, but that's what happens when a parent buys filtering software, installs it, and then walks away from their child's machine" (Gebeloff, 1999).

With laws mandating the use of various forms of censorware to meet government regulations like CIPA, and liability issues at school, the library, or work, it is no surprise that the marketplace of ideas has increasingly chan-

neled its financial resources into for-profit filtering products. Companies easily win over school and library administrators by guaranteeing adherence to government legislation as well as liability protection and parental approval. For $14.95, SafeSurf markets *Safe Eyes* as an effective tool that "uses the N2H2 website database which has been proven time after time to be the most accurate database available . . . In recent tests, both the U.S. Department of Justice and the Kaiser Family Foundation found N2H2 to be the best" (SafeSurf, 2004b). Official endorsements from prominent governmental, industrial, and educational groups are an added selling point, such as N2H2's official stamp of approval from the American Library Association for meeting CIPA rules.

As for the pervasiveness of filtering products, a poll conducted as early as 1998 at the Technology + Learning conference revealed that 51 percent of surveyed teachers, technology directors, school board members, and other educators had adopted some form of censorware for all or some students in their district (cited in Kongshem, 1998). Another poll conducted in 2000 by MSNBC.com found that "many users rely on an Internet service provider, or ISP, to do the filtering for them. The big names in this market are America Online, The Microsoft Network, Mayberry USA, Rating-G Online and Getnetwise.com. Filters that are popular with Christians and conservatives include Family.Net, Integrity Online and Hedgebuilders.com" (Nodell, 2000). With no centralized board or groups to review the practices of these filtering companies or ISPs for their effectiveness or appropriateness, it is easy to see how those seeking to meet the needs of their schools, libraries, work, or homes turn to various programs without clear indication of their validity and reliability, especially institutions pressured to have some "safety plan" to meet CIPA legislation or issues of liability.

Accordingly, it is no surprise that filtering producers and marketers stand to gain financially by lobbying for nongovernmental solutions to censorship, as well as a deregulatory media environment allowing telecommunications firms to continue to merge and expand their online assets and streamline Web content. MSNBC's interest in polling Internet user preferences for filtering is not purely for newsworthiness given its partnership with Microsoft. The same is true for AOL Time Warner. What is more, in addition to cornering the market for libraries, schools, and homes, many of these companies have ventured into the work environment. As MSNBC.com reporter Bobbi Nodell explains, "many filter companies are moving into the corporate market, which is booming because employers are concerned about workers 'wasting time' on the job and want to keep them from shopping, checking investments and playing games . . . the corporate market is expected to grow from $60 million in 1999 to $500 million in 2004" (Nodell, 2000).

Confirmation of this trend can be found with Net Nanny. Looksmart, a leading business firm in online search technology, recently acquired Net

Nanny for approximately $5 million in cash and stock in April 2004. Indeed, in their ability to promote and streamline commercial content (while limiting "inappropriate" sites), monitor Internet user habits, profile users for direct marketing purposes, and market products to users, filtering software products can be considered stepchildren of the highly lucrative commercial search engines, which became the most lucrative Web properties in 2003 due to their increasing ability to promote commercial Internet content. As LookSmart CEO Damian Smith stated in 2004:

> This acquisition is both strategic and prudent for LookSmart . . . Strategic, because integrating our search technology into Net Nanny provides a stronger product for their users, while also providing LookSmart with a desktop platform from which to launch high margin search and paid listings applications. Prudent, because Net Nanny is expected to produce positive margin contributions for LookSmart in 2004. (LookSmart, 2004)

In other words, this partnership, along with MSN funding, will allow LookSmart to apply its tracking and marketing capabilities to Net Nanny's software and related proprietary environments. As the company explains to its shareholders, such a partnership "will enhance the leading online filtering software and provide high-quality proprietary search traffic for LookSmart."

While filtering technology continues to thrive in the Internet's "free market" system, and as Web content continues to grow exponentially, the profits for filtering technology continue to expand commercially. Net Nanny's acquisition by LookSmart makes clear that one of the leading "protectors" of illicit online content is poised to become a predator of tracking and marketing to today's Internet users as it shifts its mission to "high margin search and paid listings applications" (LookSmart, 2004). With substantial profit predictions for filtering companies expanding their business within the corporate market, the goals to protect Internet users, including children, are becoming further marginalized at a time when schools, libraries, and businesses are becoming increasingly dependent upon filtering technology.

To make matters worse, "the Internet's status as an open forum for ideas" has come under attack since 2002 with a Federal Communications Commission (FCC) ruling that shields cable companies from having to open their networks to smaller competitors and civil liberties and consumer advocacy groups (Wolverton, 2002). As Karen Charman (2002) explains, "without public policies mandating open access," cable will monopolize broadband width, denying access to other Internet Service Providers in order to capitalize off of hyper-commercialized services that make it easier to buy products. Troy Wolverton (2002) of ZDNet news explains that "lack of competition among cable Internet providers could be a form of censorship . . . even if they don't completely block Web sites, cable companies

could slow access to them to the point that they become all but impossible to reach . . . while they could speed access to their own sites and those of preferred partners." Subsequently, if "the Internet content accessed by K-12 youth is patrolled by capitalist institutions, rather than by the government, educational institutions, public libraries or communitarian groups, it will inevitably become more difficult 'to turn the one-way system of commercial media into a two-way process of discussion, reflection, and action'" (Thoman, 1998, p. 3). As Resnick explains, no matter how well conceived or executed, any labeling or blocking system will tend to stifle noncommercial communication since the time and energy needed to label will inevitably lead to many unlabeled sites: "Because of safety concerns, some people will block access to materials that are unlabeled or whose labels are untrusted. For such people, the Internet will function more like broadcasting, providing access only to sites with sufficient mass-market appeal to merit the cost of labeling" (Resnick, 1997, p. 106). This form of censorship is a serious problem as the possibilities for a decentralized and openly available information network will once again be delimited by a top-down capitalist hierarchy where nondominant, noncommercial, or alternative sources of information will remain peripheral.

Finally, information filtering does not prepare students to learn how to analyze and evaluate information once they are no longer using the Internet within an educational setting. This point has gained momentum as media literacy educators, librarians, and scholars have been grappling with the need for solid media literacy curricula that include a critical and analytical approach to learning with and about online communications technology (Fabos, 2004; Frechette, 2002; Paxson, 2004; Tyner, 1998).

Testing Content Controls for Cyber-Capitalism

The hegemonic impulse of online safety profiteers becomes clear when we take a look at some ratings organizations, online proprietary environments, ISPs, and databases recommended by parents, the government, educational institutions, and the industry. First is SafeSurf, a rating organization that claims to be "dedicated to making the Internet safe for your children without censorship." Through an information database of objectionable sites, a proprietary environment for children, and safety tools for parents, SafeSurf believes they "will enable software and hardware to be developed that will enable more effective use of the Internet for *everyone*" (SafeSurf, 2004a, emphasis added).

My skepticism about claims that "everyone" benefits through SafeSurf's methods developed when visiting the SafeSurf home page, where I reviewed their policies, claims, and method to create an environment that is child tested and parent approved. What first drew my attention to their Web site were the various advertisements centered on the page. One ad displayed a large colorful rectangle for Card Service Online, "the leader in online

real time credit card processing," featuring Mastercard, Visa, Discover, and American Express. Directly under it was an ad for *Child Magazine,* on sale at the reduced price of $7.95; its pitch: "One year for the price of a bottle." Beneath this was a bold advertisement link to "Update Microsoft's Internet Explorer to support SafeSurf Ratings." Combined, these ads validated my forewarning about the interconnections between powerful computer firms, such as Microsoft, and blocking software products.

My findings led me to presume that more advertising would emerge on the *SafeSurf Wave* link, which offers *Kid's Wave,* a list of "top sites" purportedly "devoted to educating and entertaining children." On the *Kid's Wave* front page, I was informed "There are great places to take your children online." Below was a grid of partial listings of SafeSurf-approved sites by category. The first category was the "favorite site of the month," which was *Squigly's Playhouse.* By clicking on the cartoon graphic, my hypothesis was reaffirmed: the unfolding visual displayed a large color advertisement for Disneyland with moving graphics and a photo of the Magic Kingdom. The flashing text read "[frame 1: photo and text depicted Disneyland Resort] To really enjoy yourself here; [frame 2: photo of Mickey Mouse described as 'the Disneyland Trip Wizard'] Pick up your custom schedule here."

In case the ad was overlooked, each separate clickable *Kid's Wave* link for an activity or game was infused with the Disney Resort campaign. For instance, the "Squigly's Games" page had another large, flashing, color ad for Disney at the top that read, "[frame 1: photo of Mickey Mouse] Are you the Ultimate Disney fan?; [frame 2: photo of Goofey] Click here—enter to win"; on the bottom, a three-frame flashing ad targeted at parents read, "[frame 1] You know what you put on your card; [frame 2] but do you know what *he* put on your card? [picture of a crowd with a man circled in red]; [frame 3] Find out with your free credit report online." Other pages, like "Squigly's Writing Corner" or "Brainteasers," featured separate Disney ads as well as credit card ads (presumably targeted at parents, but also at a new generation of consumers).

Disney, it seems, is a frequent advertiser on filtering software products. In addition to selling nonsoftware products, such as $40 embroidered golf shirts, Net Nanny's Internet Web site had an advertisement for Disneyland featured on its front page. Most troubling, however, is that advertising clients are also the sponsors of Net Nanny content. Among its "safe-sites" for kids were "fun" links to Disney, Crayola, and Kids Channel. Under the category "Education" was a Colgate "Kidsworld" link with prominent product advertisements for Colgate toothpaste. Describing its mission in philanthropic terms, Colgate Palmolive Co. purportedly maintains the Internet site "as a service to the Internet community." A closer look at the page proves otherwise. First, I had to type in my first name and specified password of the day, "toothpaste," in order to enter the "No Cavities Clubhouse." There, I was greeted by "Dr. Rabbit" who appeared in his

clubhouse holding a toothbrush and Colgate toothpaste. Although this Web site offered "interesting oral care facts, games, and stories aimed at raising children's awareness of oral health," I could not get away from Dr. Rabbit and his *Colgate* endorsement no matter what activity I clicked on. Moreover, in spite of its "intention" to adhere to the Children's Advertising Review Unit (CARU) Guidelines for advertising on the Internet and online services, my name and email were still requested so that the "Tooth Fairy" could send me an email message—no doubt carrying her Colgate toothpaste and brush in cyber-flight.

Although not nearly as plastered in advertising as SurfWatch or Net Nanny, CyberPatrol's Web site unquestionably catered to/partnered with commercial Web sites, including Disney's Internet empire of kid-targeted Web addresses. A recommended "safe" site was "*Toy Story* Games," a game developed by Disney based on its *Toy Story* movie. Not surprisingly, Disney's home page was saturated with child and adult-directed advertising. Although the advertising contained here was "2nd level," meaning that I had to click on the recommended sites before being inundated with ads, the sites contained on the page remained uncontested as child appropriate.

As evidenced within these kid-designated Web sites, the far-reaching clutches of advertisers are rendered invisible in the discourse or underlying rationale of Internet protectionism. While children are deemed to be impressionable when it comes to sex, pornography, adult content, and nefarious language, concerns about manipulative advertising campaigns go largely undetected within "kid-safe" Internet domains.

Conclusion

Media literacy scholar Len Masterman's explanation of critical autonomy, to "develop in pupils enough self-confidence and critical maturity to be able to apply critical judgments to media texts *which they will encounter in their future*" (1985, p. 24; emphasis added), does not fit within the logic of commercial filters and the self-regulated corporations attempting to control and streamline Internet content. As Elizabeth Thoman (1998) clarifies, "the media have become so ingrained in our cultural milieu that we should no longer view the task of media education as providing 'protection' against unwanted messages." Hence, a learning model of awareness, analysis, reflection, action, and experience leads to better comprehension, critical thinking, and informed judgments.

Contrary to filtering mechanisms designed to censor or reduce student exposure to "inappropriate" Web sites and online information, a much better approach toward new information technologies is to go beyond teaching students about how to use computers, email, Web browsers, etc. First and foremost, the goals of media literacy must go hand in hand with computer training and online access through the instruction of critical skills by which students learn to discriminate all types of information. While there are

hazards to over-regulation and under-regulation of the Internet, educators and librarians have an important role to play in developing online media literacy initiatives so that students can become discerners of the types of information they need. The goals for taking media literacy to the Internet must go beyond the critical evaluation and use of information to include an analysis and understanding of the impact of political and economic forces that drive and control much of the Internet. Within a "media literacy in cyberspace" model, the issues of ownership, profit, control, and related effects are essential to helping students formulate constructive action ideas that will lead to their own Internet choices and surfing habits (Frechette, 2002). As PICS chairman Paul Resnick (1997) admits, "no labeling system is a full substitute for a thorough and thoughtful evaluation." In the end, if the power of Internet content labeling, ratings, and restrictions are left to a third party or profit-making companies, then educators, librarians, and parents need to lobby that they serve the *public* interest rather than private commercial interests.

Note

1. For example, AT&T, Dell Inc., Microsoft, Verizon, America Online Inc., American Library Association, Amazon.com, Center for Democracy & Technology, Comcast, Earthlink Inc., Recording Industry Association of America, Visa USA, Wells Fargo, and Yahoo!

References

AOL. (2004). *Welcome to AOL@School.* Retrieved December 1, 2004, from http://www.aolatschool.com.

Carlson, C. (2002). Patrolling the cyber-borders. *Eweek.* Retrieved December 1, 2004, from http://www.eweek.com/article2/0,1759,1654902,00.asp.

Charman, K. (2002). Recasting the Web: Information commons to cash cow. *Extra!: Newsletter of Fairness and Accuracy in Reporting.* Retrieved December 1, 2004, from http://www.fair.org/extra/0207/open-access.html.

Commercial Alert. (2000). Coalition asks states to protect children from ZapMe! [News release]. *Commercial Alert.org.* Retrieved December 1, 2004, from http://www.commercialalert.org/index.php/category_id/2/subcategory_id/40/article_id/63.

Commercial Alert. (2003). Commercial Alert Asks FCC, FTC to require disclosure of product placement on TV. *Commercial Alert.org.* Retrieved December 7, 2004, from http://www.commercialalert.org/index.php/article_id/index.php/category_id/1/subcategory_id/7/article_id/193.

ConsumerReports.Org. (2001). Digital chaperones for kids: Which Internet filters protect the best? Which get in the way? *Consumer Reports.* Retrieved December 1, 2004, from http://www.consumerreports.org/main/detail.jsp?CONTENT%3C%3Ecnt_id=18867&FOLDER%3C%3Efolder_id=18151.

Fabos, B. (2004). *Wrong turn on the information superhighway: Education and the commercialization of the Internet.* New York: Teachers College Press.

Federal Bureau of Investigation. (2004). *A parent's guide to Internet safety.* Retrieved December 1, 2004, from http://www.fbi.gov/publications/pguide/pguidee.htm.

Federal Trade Commission. (2004). *Hearing on online pornography: Closing the door on pervasive smut.* Washington, DC: U.S. Government Printing Office.

Frechette, J. (2002). *Developing media literacy in cyberspace: Pedagogy and critical learning for the twenty-first-century classroom.* Westport, CT: Praeger Publishers.

Gebeloff, R. (1999). Screening zone: The trouble with net filters and ratings. *Money Talks.* Retrieved December 1, 2004, from http://www.www.prnewswire.com/cgi-bin/stories.pl?ACCT=105&STORY=/www/story/9–15–97/316603.

GetNetWise. (2004). AT&T. *GetNetWise.* Retrieved December 1, 2004, from http://www.getnetwise.org/about/supporters/att.

Gramsci, A. (1971). *Selections from the prison notebooks.* New York: International Publishers.

Grossman, M. (2000). Living with the Children's Online Privacy Protection Act. *Gigalaw.com.* Retrieved December 1, 2004, from http://www.gigalaw.com/articles/2000–all/grossman-2000_06–all.html.

Hill, L. (2000). Second coming of cyberangels. *Wired News.* Retrieved December 1, 2004, from http://www.wired.com/news/culture/0,1284,35279,00.html.

Internet Content Rating Association (ICRA). (2004). *About ICRA.* Retrieved December 1, 2004, from http://www.icra.org/about/.

Jules, V. (2004). *Supreme Court finds SafeSurf's solution is better than COPA* [Press release]. Retrieved December 7, 2004, from http://www.safesurf.com/press/press28.htm.

Kongshem, L. (1998). Censorware: How well does Internet filtering software protect students? *Electronic School Online.* Retrieved December 7, 2004, from http://www.electronic school.com/0198f1.html.

LookSmart (2004, April 29). *LookSmart acquired Net Nanny.* Retrieved July 14, 2004, from http://www.shareholder.com/looksmart/releaseDetail.cfm?ReleaseID=134151

Masterman, L. (1985). *Teaching the media.* London: Comedia.

Munro, J. (2004). Cybersitter 9.0 [Electronic version]. *PC Magazine.* Retrieved December 7, 2004, from http://www.pcmag.com/article2/0,1759,1618830,000.asp.

N2H2. (2004). *Secure computing.* Retrieved December 7, 2004, from www.n2h2.com/products/index.

Net Nanny. (2004). Home page. Retrieved December 7, 2004, from http://www.netnanny.com.

Nodell, B. (2000). Filtering porn? Maybe, maybe not: Shielding kids from the Web's dark side isn't a science yet. *MSNBC.com.* Retrieved December 7, 2004, from http://www.msnbc.com/news/438174.asp?cp1=1.

Ochoa, E. (2003). Protecting children from the dangers of instant information. *News8Austin.com.* Retrieved December 7, 2004, from http://www.news8austin.com/content/news_8_explores/modern_day_parenting/?SecID=324&ArID=71196.

Paxson, P. (2004). *Media literacy: Thinking critically about the Internet.* Lincoln, NE: GPN Educational Media.

Phillips, P., & Project Censored. (2001). *Censored 2001: The year's top 25 censored stories.* New York: Seven Stories Press.

Resnick, P. (1997). Filtering information on the Internet. *Scientific American,* March, 106–108.

Rubin, S., & Lamb, M. (1997). *Internet/online summit highlights cooperation and action to enhance the safety and benefits of cyberspace for children and families.* Retrieved December 7, 2004, from http://www.kidsonline.org/news/advisory_971202a.html.

SafeSurf. (2004a). *Home page.* Retrieved December 7, 2004, from http://www.safesurf.com.

SafeSurf. (2004b). SafeEyes. *SafeSurf.com.* Retrieved December 7, 2004, from http://www.safesurf.com/filter/safeeyes.htm.

Schiffman, B. (2000). ZapMe kills computers in the classroom. *Forbes.com.* Retrieved December 7, 2004, from http://www.forbes.com/2000/11/28/1127zapme.html.

Shyles, L. (2003). *Deciphering cyberspace: Making the most of digital communication technology.* Thousand Oaks, CA: Sage.

Silver, D., & Garland, P. (2004). "Shop online!": Advertising female teen cyberculture. In P. Howard and S. Jones (Eds.), *Society online: The Internet in context* (pp. 157–171). Thousand Oaks, CA: Sage.

Thoman, E. (1998). *Skills and strategies for media education.* Retrieved December 7, 2004, from http://www.medialit.org/reading_room/pdf/CMLskillsandstrat.pdf.

Trotter, A. (2001). New law directs schools to install Internet filtering devices. *Education Week, 20*(16), 32.

Tyner, K. (1998). *Literacy in a digital world: Teaching and learning in the age of information.* Mahwah, NJ: Lawrence Erlbaum Associates.

U.S. Census Bureau. (2001). *Home computers and Internet use in the United States.* (Report No. P23–207). Washington, DC: U.S. Government Printing Office.

Williams, T. (2003). AOL@SCHOOL expands its free online learning service with new alliances

and expanded relationships with industry leaders [Electronic version]. *Business Wire*. Retrieved December 7, 2004, from http://www.findarticles.com/p/articles/mi_m0EIN/is_2003_Oct_23/ai_109171992.

WiredSafety. (2004). Home page. Retrieved December 7, 2004, from http://www.wiredsafety.org.

Wolverton, T. (2002). Accounting options: A new tech order. *ZDNET News*. Retrieved December 7, 2004, from http://news.zdnet.com/2100–9595_22–947159.html.