Controlling Access to the Internet: The Role of Filtering

R. S. Rosenberg
Department of Computer Science
University of British Columbia
Vancouver, BC Canada V6T 1Z4
604-822-4142
604-822-5485 (FAX)
rosen@cs.ubc.ca

Abstract

Controlling access to the Internet by means of filtering software has become a growth industry in the U.S. and elsewhere. Its use has increased as the mandatory response to the current plagues of society, namely, pornography, violence, hate, and in general, anything seen to be unpleasant or threatening. Also of potential concern is the possible limitation of access to Web sites that discuss drugs, without distinguishing advocacy from scientific and informed analysis of addiction. With the rise of an effective creationist movement dedicated to the elimination of evolutionary theory in the curriculum, it is to be expected that attempts will be made to limit access to sites presenting such theories, in certain jurisdictions in the U.S. The current preferred method of choice to limit access is to filter content either by blocking access to specific Web sites, referred to by their URLs, or by using a large set of keywords to prevent accessing sites that contain one or more of these words. Another more insidious scheme is to encourage or even require every Web site to rate its content along a number of dimensions, including violence, language, sexual explicitness, and nudity. Then individual browsers can be programmed to return references only to those sites that fall below a pre-specified profile. The dangers for free speech inherent in such schemes will be discussed. Efforts to produce legislation in the U.S. to mandate the use of filtering or rating programs will be described, as will some recent court decisions involving their use in libraries.

Free Speech, Filters, Internet, Libraries, Ethics, United States

INTRODUCTION

Controlling access to the Internet by means of filtering software has become a growth industry in the U.S. and elsewhere. Its use has increased as the mandatory response to the current plagues of society, namely, pornography, violence, hate, and in general, anything seen to be unpleasant or threatening. On the legislative agenda is the limitation of access to any Web sites that discuss drugs, without distinguishing advocacy from scientific and informed analysis of addiction. (Pending Bills, 2000) With the rise of an effective creationist movement dedicated to the elimination of evolutionary theory in the curriculum, it is to be expected that attempts will be made to limit access to sites presenting scientific evolutionary theory, in certain jurisdictions in the U.S.

In this paper, the various strategies incorporated within current filtering programs are briefly described as well as the apparent content issues on the Internet that motivate their use both in private and public contexts. Underlying this motivation is a mixture of political and social pressures to take action against real and perceived problematic Internet content. This motivation has manifested itself in proposed and enacted legislation and also a number of lawsuits. Some of these are reviewed and serve to support the present viewpoint against the mandatory use of filtering programs in libraries and community centers among other public places. My focus is on the U.S. because the issues of concern are the subject of legislative actions and are topics of widespread analysis and debate. In another paper on filtering, (Rosenberg, 1999) the focus was placed on how librarians deal with their professional responsibility to provide open access to information as well as their social responsibility to the members of their community, young and old alike. The players are many and varied - concerned individuals and families, librarians, library and school boards, state legislators, judges, congressman, senators, religious groups, civil liberties groups, Internet advocates, and of course the media - and their motives are not always transparent. As with many other issues that mingle politics and morality, the story of filtering is both new and somewhat familiar.

To fully appreciate the magnitude of the problem facing those who wish to regulate the World Wide Web, its current size (roughly) and its growth rate (also roughly) should be known. Fortunately, recent statistics are available from the OCLC (Online Computer Library Center), a research organization that aims to “further (the public's) access to the world's information and reduce information costs.” OCLC reported results of its June 1999 survey during September 1999 (June 1999 Web Statistics, 1999). The total number of unique Web sites was estimated as almost 3.7 million, with almost 2.23 million being public, 389,000 private and just over a million provisional. These numbers are estimated to vary in accuracy between +/- 3% to +/- 10%. The public sites were estimated to contain almost 290 million pages (+/- 35%). The rate of growth of unique public sites is quite large: 179% between 1997 and 1999. The Web is very large and getting larger at a high rate. This growth rate raises many issues of access because to be accessible by search engines, pages must be scanned and catalogued as they come online.

There is, however, no consensus on Web statistics. In a famous paper published in *Nature*, (Lawrence and Lee, 1999), the number of public Web sites, as of February 1999, was estimated to be 2.8 million. The number of indexable pages was estimated as 800 million, more than two and one-half times the figure given above. The results are based on a complete examination of the first 2,500 random web servers discovered. In addition, Lawrence and Lee manually classified the content of these servers and reported that "about 83% of servers contain commercial content (for example, company home pages)." The remaining 17% is made up of scientific/education (6%), pornography (1.5%), government (1.2%), health (2.8%), personal (2.3%), community (1.4%), religion (.8%), and societies (2%). Note that some sites have multiple classifications. No criteria are given for these categories, except for scientific/education. Based on this paper, there are 1.5 million pornographic pages, although the defining terms are unknown. Depending on one's point of view, this is a large number or a small one.

In the next section, various concerns related to the use of filtering and blocking strategies will be described and discussed, as well as the different strategies employed in their use. In the section on legal and legislative consideration, the current state of the law in the U.S. is discussed and a number of pending bills in the U.S. Congress designed to mandate filtering in public libraries and schools are described. Finally, the position taken in this paper is summarized and supporters of free speech and open inquiry are urged to renew their efforts to defend these freedoms.

FILTERS: TECHNICAL, LEGAL, AND SOCIAL CONCERNS

Filters are programs that are designed to restrict access to Web sites, newsgroups, and chat rooms by a variety of techniques. In this section, a few definitions will be provided, a few problems with filters will be articulated, and reasons for advocating the use of filters presented.[1]

How Do Filters Work?

It is important to distinguish among different strategies for limiting access to Web sites and newsgroups. The simplest approach is to compile a list of URLs and newsgroups that are to be blocked. Such a list must be continuously updated given the dynamic growth of the Internet. A substantial number of individuals must be employed to perform this function and must operate under an agreed upon and closely followed set of guidelines. Such filters require that users regularly download the updated banned site list and simply adopt it because of the near impossibility of evaluating its quality or determining whether or not it meets their concerns. For some filters, users can add newly discovered unacceptable sites to the banned list. The default strategy is to accept the judgment of others, namely, profit-making corporations subject to marketplace pressures in determining which sites are off-limits.

Another strategy is to compile a list of English keywords, which characterize the material in Web sites that is judged unacceptable for viewing. This list can be regularly modified to reflect more precise descriptions or new concerns. Keywords, even Boolean combinations of keywords, are a rather poor representation of the

[1] Among the vigorous advocates of filtering in public libraries are Dr. Laura Schlessinger (http://www.drlaura.com/), who seems to believe that the American Library Association is interested in pandering pornography to children and David Burt, a librarian and president of Filtering Facts (http://www.filteringfacts.org), Visits to these site are quite informative.

meaning of texts and therefore may block otherwise acceptable sites. Their attraction is that they give the appearance of effectiveness because if it is desired to block access to sites containing documents and graphics, dealing with naked women, such keywords and Boolean forms as nudity, naked, nudity AND women, and naked AND women, should be effective.

The last general category of blocking or filtering strategies is similar to systems used to rate music on CDs and cassettes, movies, and television shows. Simply put, Web sites would be expected to rate their content along several dimensions including sexual explicitness, nudity, violent language and violent graphics. The ratings, on simple numeric scales, can be combined into a profile that characterizes, for a given user, an envelope for acceptable sites. For example, if a site's ratings exceed the profile along even one dimension, that site will be blocked by the browser. Such a system requires, among other things, that sites rate themselves, that such ratings accurately reflect content, a non-trivial task subject to legitimate disagreements, and that disagreements on ratings be adjudicated by some impartial board. Also it is necessary that sites rate themselves, for a default condition must be that non-rated sites are automatically blocked. There is more, much more about the possible repercussions of self-rating systems.

The following definitions (Hocheiser, 1998) are taken from the CPSR (Computer Professionals for Social Responsibility). CPSR is an activist organization concerned with a variety of social issues associated with the use of computers.

> A **content filter** is one or more pieces of software that work together to prevent users from viewing material found on the Internet. This process has two components.
>
> **Rating**: Value judgments are used to categorize web sites based on their content. These ratings could use simple allowed/disallowed distinctions like those found in programs like CyberSitter or NetNanny, or they can have many values, as seen in ratings systems based on Platform for Internet Content Selection.
>
> **Filtering**: With each request for information, the filtering software examines the resource that the user has requested. If the resource is on the "not allowed" list, or if it does not have the proper PICS rating, the filtering software tells the user that access has been denied and the browser does not display the contents of the web site.

In somewhat more detail, the American Library Association, responds to the question, What is Blocking/ Filtering Software? as follows: (American Library Association, 1997)

> Blocking/filtering software is a mechanism used to:
>
> - restrict access to Internet content, based on an internal database of the product, or;

- restrict access to Internet content through a database maintained external to the product itself, or;
- restrict access to Internet content to certain ratings assigned to those sites by a third party, or;
- restrict access to Internet content by scanning content, based on a keyword, phrase or text string or;
- restrict access to Internet content based on the source of the information.

Finally, the following definition of PICS (Resnick, 1997) describes the functioning of a system based on a rating mechanism:

> The Massachusetts Institute of Technology's World Wide Web Consortium has developed a set of technical standards called PICS (Platform for Internet Content Selection) so that people can electronically distribute descriptions of digital works in a simple, computer-readable form. Computers can process these labels in the background, automatically shielding users from undesirable material or directing their attention to sites of particular interest. The original impetus for PICS was to allow parents and teachers to screen materials they felt were inappropriate for children using the Net. Rather than censoring what is distributed, as the Communications Decency Act and other legislative have tried to do, PICS enables users to control what they receive.

These definitions are not exhaustive, of course, but are suggestive of a wide range of actual products comprising a very competitive marketplace. The general public in North America seems to be convinced that there exists a serious problem with respect to the access of offensive material on the Internet and that filters are the best solution.

Content that Motivates Concerns

Who wants to regulate Internet content and limit access as well? Many parents are fearful of allowing their children unsupervised access to the Internet because of personal experiences in discovering unacceptable material for young children and also because of a continual stream of newspaper and television reports that frequently highlight the worst of the Internet. For example, Pamela Mendels, of the New York Times, reports the following (Mendels, 1999a):

> A new survey of teachers at public schools that are online found, for example, that 58 percent of the respondents reported that Internet access at their schools was filtered. That was an increase from the 38 percent of teachers who reported filtered access last year, according to Quality Education Data, a Denver-based education market research company. The company surveyed 403 teachers in schools across the country.

> Meanwhile, almost a third of online American households with children use blocking software, according to another study published recently. In a poll of parents of minors with Internet access at home, the Annenberg Public Policy Center of the University of Pennsylvania found that 31 percent used filtering devices.
>
> The same study also found that parents have mixed feelings about the Internet. More than 80 percent said their kids used the Internet to help with homework and that the global network allowed them to "discover fascinating useful things." But 77 percent also said they feared that children would give out personal information online and 60 percent said that too much time online could lead children to become more isolated from others. Perhaps most significant, 60 percent of respondents said they disagreed with the statement that the Internet was a safe place for their children.

Other findings of interest appear as follows in the report itself, (Turow, 1999):

> • Most parents with online connections at home are deeply fearful about the Web's influence on their children. Online parents can be categorized as online worriers, disenchanteds, and gung ho's. The gung ho group, the only one with overall positive attitudes, makes up only 39% of online parents.
> • 32% of parents with online connections use protective software that guards children's access to sites, a sign that a substantial number of parents have gone out of their way to try to deal with the concerns they hold.

Summarizing the findings in the survey, the author characterizes the existing fears that most parents share:

> Parents are nervous about two features of Web programming they haven't seen in broadcast or cable television: its wide-open nature and its interactivity. Parents fear the Web for its unprecedented openness - the easy access by anybody to sexuality, bad values, and commercialism. They also fear the Web for its unprecedented interactive nature - the potential for invading a family's privacy and for adults taking advantage of children. These fears are heightened among many parents because they don't believe they understand the technology well enough to make the best use of it. Yet they believe their children need it.

Thus, the apprehension that parents feel about this new technology provides fertile ground for efforts to regulate, control and restrict access to the Internet. Politicians, law enforcement officials, certain religious groups, and others, with apparently genuine concerns about the welfare of children, are willing and even eager to treat the Internet as hostile territory. Complicit in this situation is the media that have consistently presented the Internet as both revolutionary and dangerous. Witness Turow's review of some of the media's proclivities with respect to the reporting of Internet events, in which he notes that, "Overall, though, the Web presented the Internet as a Jekyll-and-Hyde phenomenon over which parents are left to take control with little community backup." Consider the following findings of the extensive survey conducted for this study:

> • Sex crimes regarding children and the Web were featured in one of every four articles. The most common crime topics were sexual predators and child pornographers.
> • Disturbing issues relating to the Web and the family showed up in two of every three articles surveyed. The problems portrayed were rather narrow - mostly sex crimes, pornography, and privacy invasion.
> • Benefits of the Web for the family came up in half the total articles, but there was little overlap with the negative pieces. The dangerous world of the Internet and the friendly, useful picture of cyberspace showed up in different articles and were unrelated to each other.
> • When articles quoted people about the Internet and the family, many more sources stressed the dangers of the Web than its benefits. Government officials and law enforcement officers spoke most frequently, and most negatively, about the Web's influence on children and the family. Educators were mostly positive, but they showed up only rarely.
> • Because of the focus on crime, reporters looked often to the government and criminal justice system for remedies. The solutions they represented were typically either piece-meal (for example, arresting an individual child-pornography suspect) or muddled and tentative (such as court-voided legislation to protect children from Web indecencies).

A recent update of this survey shows that not much has changed.[2]

Shortly after the first of the previously mentioned surveys appeared, the software company Websense, which just happens to produce filtering programs, announced the results of study that it had commissioned. The following highlights appeared in (Lazarus, 1999):

[2] This assessment that the Internet is not an interesting luxury but a near necessity is undercut, however, by concerns. For example:
• About seven in 10 parents (71%) in 2000 agree with the statement "I am concerned that my children might view sexually explicit images on the Internet." Seventy-six percent agreed with this in 1998.
• 51% (compared to 48%) agreed that "families who spend a lot of time online talk to each other less than they otherwise would."
• Sixty-two percent of parents agreed with the new statement this year "I am concerned that my children might view violent images on the Internet." (Turow and Nir, 2000)

> Software company Websense commissioned a survey last month and was shocked, shocked, to discover that lots of kids visit “objectionable” Web sites while surfing the Net at school. . .
>
> “Maybe it's obvious,” Ted Ladd, the company's public relations manager, said of the survey results. “But it's good for people to know what's happening in schools.”
>
> What's happening, according to a survey of 501 teenagers ages 13 to 17, is that 58 percent of young Web users admit to having visited sites containing sexual content, violence, hate material or “music that might offend people” while using Internet-connected school computers.
>
> This may come as something of an eye- opener to the 173 parents who also participated in the survey. Fully three-quarters said they know “everything or a fair amount” about how their kids spend time on the Net. . . .
>
> Websense claims that its own filters are in use at about 2,500 schools nationwide. But just to be on the safe side, it's sending out free copies with summaries of the survey to hundreds of others.

It does not seem inappropriate to say that the results of this study are both unsurprising and self-serving. What else do kids do online in addition to seeking out and viewing “objectionable” material? Perhaps they shop, make new friends, or maintain friendships. A survey titled, “Kids Online (1999),” reports just these results:

> It shows that the impulse toward e-commerce starts at an early age. For example:
>
> • One out of six kids are allowed to make purchases on the Internet.
> • One in seven has actually done so.
> • 52% of the children surveyed had asked their parents to buy something they saw on the net.
> • 46% of the parents said they had been asked to buy something.
> . . .
> That 42% have subscribed to a website or other service online indicates an area of potential concern. This is despite the fact that nearly 85% of parents have rules against doing so, and 80% of children say they know these rules. Another issue is who they meet online:
> • Roughly 50% of the children had met a new friend online, a figure that was equally true for boys and girls.
> • 42% of parents knew that their children had made friends online.

If the Internet is unsafe for kids, as many parents clearly believe, but the growth of E-commerce requires making it a safe place, then filtering as part of an overall business strategy makes sense. Furthermore, it has the distinct advantage of seeming to place the necessary power in the hands of parents and local officials, not in the federal government's, except for certain special cases such as child pornography. So whether it is the issue of personal privacy or Internet content, the predominant marketplace position is self-regulation. Nevertheless, as we shall see, the US federal government has shown itself to be very interested in mandating the use of filters to protect children wherever federal money is involved in facilitating Internet access.

One recent instance of this business view was a conference sponsored by the Bertelsmann Foundation, funded by a very large, German-based, international media company, in Germany last September. Presented at the conference was a memorandum, prepared under the leadership of an international team. Its title is not at all surprising, namely, “Self-regulation of Internet Content (1999).” The key recommendations of this report are interesting in light of the foregoing discussion and although the list is long, it does reveal the motives of a major segment of the marketplace.[3] Self-regulation is good; government action or legislation is bad. Filters

[3] **1. The Internet: changing the way people live**
The Internet will change the way people live: it offers extraordinary opportunities for enhancing creativity and learning, for trading and relating across borders, for safeguarding human rights, for realizing democratic values and for strengthening pluralism and cultural diversity. . . Mechanisms have to be developed to deal with illegal content, to protect children online as well as guarantee free speech.

2. Self-regulation of Internet content: towards a systematic, integrated and international approach
No single approach, relying on one form or one set of actors, can provide a solution to content concerns in the changing and shifting environment that is the Internet. . . Given the global and borderless architecture of the Internet, such a systematic approach requires not only coordination at a national and regional level, but its scope must be international.

3. Internet industry: developing and implementing codes of conduct
As part of the codes of conduct, Internet providers hosting content have an obligation to remove illegal content when put on notice that such content exists. . . It is in the best interest of industry to take on such responsibility since it enhances consumer confidence and is ultimately good for business.

4. Sharing responsibility: self-regulatory agencies enforcing codes of conduct
To be effective, codes of conduct must be the product of and be enforced by self-regulatory agencies. Such agencies must be broadly representative and accessible to all relevant parties.

5. Governments: supporting and reinforcing self-regulation
Self-regulation cannot function without the support of public authorities, be it that they simply do not interfere with the self-regulatory process, be it that they endorse or ratify self-regulatory codes and give support through enforcement.

6. Self-rating and filtering systems: empowering user choice
Filtering technology can empower users by allowing them to select the kinds of content they and their children are exposed to. Used wisely, this technology can help shift control of and responsibility for harmful content from governments, regulatory agencies, and supervisory bodies to individuals. . . Content providers worldwide must be mobilized to label their content and filters must be made available to guardians and all users of the Internet.

7. Internet filtering: ensuring youth protection and freedom of speech
A good filtering system realizes several important values: end user autonomy; respect for freedom of expression; ideological diversity; transparency; respect for privacy; inter-operability and compatibility. . . Government or regulatory agencies may supply filters but should not mandate their use.

8. Hotlines: communicating and evaluating content concerns
We need technical and organizational communication devices to ensure that users can respond to content on the Internet that they find of substantial concern. . . Legislators should formulate minimum requirements on the organizational setup and procedures of hotlines and, in turn, shield them from criminal or civil liability incurred in the proper conduct of their business (" safe harbor").

9. International cooperation: acting against content where it is located

empower parents; otherwise, children are victimized by the surfeit of dangerous content. A satisfactory international ratings scheme is feasible and indeed necessary. Government action is also necessary to support this effort, as is a vigilant network of ISPs. Finally, hotlines are necessary for the reporting of misidentified content and violations of the system There is more but these selections should indicate something terribly seductive about the promise that self-regulation is any guarantee against censorship. The possible results of the efforts by large multinational corporations to make the world safe for electronic commerce should not be underestimated with respect to the degree to which free and open expression and inquiry will suffer.

Problems with the Use of Filters

It has been suggested above that filters may not operate effectively because of a variety of problems. Some of these will be explored in this section but it should be realized that what is viewed as a problem by critics of filters may be hailed as a virtue by supporters. For example, the National Coalition Against Censorship offered the following non-technical descriptions of some limitations of filters (Censorship's Tools Du Jour, 1998):

- **Oversimplification**. How to distinguish "good" sex (or violence) from “bad”? Filters and labels assume that television programs and Internet sites can be reduced to a single letter or symbol, or a combination of these.
- **Overbreadth**. Ratings and filters often ignore context and, thus, inevitably exclude material that users might want to have, along with material they may not want.
- **Feasibility**. What about better descriptions of television programming and Internet sites? It sounds like a good idea, but it isn't feasible. There are thousands of television programs, content changes daily, and each new program would require a new description.
- **Subjectivity**. Any rating system that classifies or describes content is dependent on the subjective judgment of the rater.

There should be an international network of hotlines governed by a framework agreement containing minimum standards on the handling of content concerns and stipulating mutual notification between hotlines.

10. The legal framework: limitations on liability

There should be no criminal responsibility of mere access and network providers for third parties' illegal content transmissions taking place in real-time through their networks.

11. Law enforcement: cooperation and continuous training

It should be a top priority to create adequate law enforcement bodies to combat computer crime and illegal content like child pornography on the Internet.

12. A "learning system": education and constant evaluation

No self-regulatory mechanism can work independently of an education and awareness campaign. The Internet industry should develop a continuous online and off-line effort to provide general awareness of self-regulatory mechanisms such as filtering systems and hotlines.

- **Full disclosure**. Few Internet filters disclose what you lose by using them. The makers of these products claim that information is proprietary and its disclosure would provide a roadmap to objectionable material.
- **Security**. Filters and ratings give a false sense security, by suggesting that all parents need to do to protect children is to block disturbing ideas and images.

Many specific examples could be given to illustrate these limitations. Searches of British regions such as Essex and Sussex are blocked because of the inclusion of "sex" in the search keywords. Other Web sites that should not be blocked because they provide necessary and useful education about sexual matters may be blocked because it is profitable to reach a large segment of the population that objects to sex education and therefore prefers this outcome. Context can sometimes be taken into account but a system of keywords is fundamentally limited because just the occurrence of certain words or phrases rarely captures true meaning. Sites belonging to organizations that promote strong free speech viewpoints, such as the American Civil Liberties Union, have been blocked by more conservative organizations. Even objecting to the patterns of exclusion adopted by certain filtering companies may result in the critical source being added to the banned list. Thus, any sites on the Internet that host discussions, which deal with free speech issues, are very like to be restricted because they will of necessity contain filter-sensitive words. The feasibility issue is paramount given the incredible growth curve of the Web and the fact the even existing Web sites change in unpredictable ways. Employees of filtering companies who must evaluate sites for content may differ significantly from one another with respect to the criteria for acceptability.

Self-rating is becoming an increasingly favoured approach to regulating content with the existing models for rating films and television shows. Again sheer numbers present significant difficulties for such systems and fewer than 200, 000 web sites had been rated as of 1999. But the implementation of a ratings system has a serious impact on artistic limits and public expectations. One interesting example is the enunciation of the (Code of the Comic Magazine Association of America, 1971). As stated in the Preamble of this Code,

> This seal of approval appears only on comics magazines which have been carefully reviewed, prior to publication, by the Comics Code Authority, and found to have met the high standards of morality and decency required by the code.

What defines “high standards of morality and decency?” It may be helpful to read the following selected portions of the Code:

> **General Standards - Part A**
>
> 3. Policemen, judges, government officials and respected institutions shall not be presented in such a way as to create disrespect for established

> authority. If any of these is depicted committing an illegal act, it must be declared as an exceptional case and that the culprit pay the legal price.
> 4. If a crime is depicted it shall be as a sordid and unpleasant activity.
> 5. Criminals shall not be presented in glamorous circumstances, unless an unhappy ends results from their ill-gotten gain, and creates no desire for emulation.
> 6. In every instance good shall triumph over evil and the criminal punished for his misdeeds.
> 11. The letters of the word “crime” on a comics magazine cover shall never be appreciably greater in dimension than the other words contained in the title. The word “crime" shall never appear alone on the cover.
> 12. Restraint in the use of the word “crime” in titles or subtitles shall be exercised.
>
> **Marriage and Sex**
> 1. Divorce shall not be treated humorously or represented as desirable.
> 2. Illicit sex relations are not to be portrayed and sexual abnormalities are unacceptable.
> 3. All situations dealing with the family unit should have as their ultimate goal the protection of the children and family life. In no way shall the breaking of the moral code be depicted as rewarding.
>
> **Dialogue**
> 1. Profanity, obscenity, smut, vulgarity, or words or symbols which have acquired undesirable meanings- judged and interpreted in contemporary standards- are forbidden.
> 2. Special precautions to avoid disparaging reference to physical afflictions or deformities shall be taken.
> 3. Although slang and colloquialisms are acceptable, excessive use should be discouraged and whenever possible good grammar shall be employed.

Imagine applying such restrictions, and others, to the writing of books or the production of movies. How would Hemingway, Fitzgerald, Faulkner, Mailer, or Roth fare under such a system? The success of contemporary comics has depended on ignoring this Code and the associated seal of approval. Those comics that have adhered to the Code are largely distinguished by their innocuousness, their predictability, their utter lack of excitement, and their instant relegation to the dustbin. Of course, comics have been read mainly by children and the Code was supposedly devised to protect their interests, with little concern about limitations on the artistic creativity of their authors. More recently, teens and adults have been the target for a large segment of the comic book industry.

Applying a ratings system to the Internet could have similar effects in addition to a host of others, given that the Internet provides a relatively inexpensive platform for millions of individual publishers worldwide. Extensive comments and critiques have been offered by many writers and groups but for the present paper, Jonathan

Weinberg, (1997) and Lawrence Lessig, (1998), both lawyers and constitutional law professors, will be referred to. As Lessig notes, PICS is a very general approach for implementing a rating system but he cautions that,

> PICS thus comports with the values of computer science; it comports with the aim of systems design. But however virtuous PICS might be from these virtuous perspectives, it should be obvious that these are not the only norms against which the architecture of the net should be tested, nor the most important. The question we should ask instead is whether the design comports with free speech values. And in my view, PICS plainly does not.
>
> PICS is doubly neutral - neutral both about the values used to filter, and about who gets to impose the filter. But the first amendment is not doubly neutral. While the censorship of the user is certainly consistent with free speech values, governmentally enabled up-stream censorship is not. Or put differently, between two free speech architectures, one which enables user control only, and one which enables both user control, and upstream control, my argument is that the government has no legitimate interest in pushing upstream control, except in a very narrow range of cases.

Weinberg makes very clear that PICS is a very powerful technical achievement that permits ratings to be assigned by arbitrary parties, as he notes,

> Finally, the PICS documents note that ratings need not be assigned by the authors of filtering software. . . . They can be assigned by the content creators themselves or by third parties. One of the consequences of the PICS specifications is that varying groups- - the Christian Coalition, say, or the Boy Scouts- - can seek to establish rating services reflecting their own values, and these ratings can be implemented by off- the- shelf blocking software. . . .

He is very apprehensive about the feasibility of a government mandated ratings system, in one country, and more so about an international agreement, as he argues in the following:

> It may be that the only way to ensure participation in a self- rating system even in a single country (let alone internationally) would be for the government to compel content providers to self- rate (or to compel Internet access providers to require their customers to do so). It is not obvious how such a requirement would work. The drafters of such a law would face the choice of forcing content providers to score their sites with reference to a particular rating system specified in the law, or allowing them leeway to choose one of a variety of PICS- compliant ratings systems. Neither approach seems satisfactory. The first, mandating use of

> a particular rating system, would freeze technological development by eliminating competitive pressures leading to the introduction and improvement of new searching, filtering, and organizing techniques. It would leave consumers unable to choose the rating system that best served their needs. The second would be little better. Some government organ would have to assume the task of certifying particular self- rating systems as adequately singling out material unsuitable for children.

There remains a serious question, of course, whether or not such a government mandated system of elaborate ratings, incorporated into PICS filtering would be constitutional. In fact, on the international scene, the US has always been the country most resistant to agreements for regulating Web content because of First Amendment concerns. All this suggests that rating the Internet internationally is a far more difficult task than rating movies in any one country. And an international rating system must be in place to be effective in any one country because of the global nature of the Internet.

Introduction to Legal and Legislative Issues

In the effort to defeat the Communications Decency Act (CDA) of 1996, a bargain was made with the devil, whether consciously or not, by many organizations and groups opposing it. Most civil liberties organizations and a number of Internet service providers (ISPs) opposed the legislation on principle in that its implementation would most certainly result in violations of First Amendment rights, because of the vague notion of "indecent" material described in the Act. In order to argue that the actions of the federal government would be too heavy handed in controlling access, many of these organizations and companies proposed the developing technology of filtering programs, or filters, as a means of empowering parents and local officials with the technical ability to limit access to unacceptable material. This support for filters seemed to be consistent with a powerful theme in American politics that local solutions to problems were to be preferred to centralized control emanating from Washington.

It might be recalled that one of the three constitutional requirements, set by the Supreme Court, for establishing that a book or film is obscene is that it violates local community standards. This emphasis on the local is currently pervasive in many views of the balance between federal and state powers. Witness recent Supreme Court decisions. Problems clearly arise in the context of a technology, the Internet, which does not recognize borders. What does local mean on the Internet where a URL, Universal Resource Locator, simply the address for a Web page can refer to a server located anywhere in the world? The Pennsylvania judges ruling on the Community Decency Act of 1996 seemed to be persuaded both that the meaning of indecent was difficult to characterize effectively and that putting control into the hands of parents and local officials would be an effective way to deal with a contentious issue. Furthermore, the use of filters would relieve ISPs (Internet Service Providers) from the onerous responsibility of monitoring the content that they transmitted and stored, to determine whether or not it might violate a rather arbitrary standard.

When the Supreme Court upheld the lower Pennsylvania court, in June 1997, in declaring sections of the CDA unconstitutional, a joyous celebration erupted on the Internet and elsewhere but the reliance on filters would soon prove to be the new battleground for free speech. Initially, the focus was on sexual material with the goal being to prevent access to Web sites and newsgroups carrying such explicit material. It is perhaps worth emphasizing at this point that if parents wish to install filtering programs into their home computers or to take advantage of filtering services offered by Web browsers or ISPs, they are perfectly within their rights to do so. From my perspective, I would only suggest that they be informed consumers and become aware of the limitations of the various available products. The battle is joined however when public bodies install filters that prevent people from exercising their First Amendment rights in the U.S. or their Charter rights in Canada. The installation of filters into public computers, whether in libraries, community centres, or schools and universities, raises a host of issues, including free speech and access.

For the present, my argument is simply that filters are too blunt an instrument to perform the task demanded of them and that the dimensions of this task are largely determined by political and religious agendas. As various ills of society are laid at the doorstep of the Internet, restricting access becomes the obvious solution. Thus, for the advocates of filtering, too much youth violence, as evidenced by school shootings, requires limiting access to violent Web material. Similarly, in their view preventing access to sites managed by white supremacists could reduce acts motivated by hate and racism. And down the road, perhaps, other social problems could find partial remedies, it is believed by many people, by further restrictions. Filters have become the remedy of choice for many problems even though they are imperfect tools, tend towards overkill, and are subject to the arbitrary agendas of many pressure groups.

LEGAL AND LEGISLATIVE CONSIDERATIONS

Recent attempts to compel library boards to implement mandatory filters on computers connected to the Internet have been met with some resistance. The most significant of these cases is the one from Loudoun County, Virginia and it will be reviewed in some detail; other cases will be mentioned, however. Simultaneously, several attempts have been undertaken in Congress, both in this session and the last, to pass legislation that mandates the installation of filters, tied to government funding. Recent terrible events in Colorado, Illinois, California, and Texas have spurred calls for blocking access to Web sites that contain information that seems to be excessively violent, racist, and sexually explicit. Many politicians on both sides of Congress have supported such attempts for many reasons, including the fact that polls show that significant numbers of Americans believe that the Internet is a dangerous place. Recall the previous discussion. Some of these bills in progress will also be reviewed.

Recent Legal Decisions

Mainstream Loudoun, et al. v. Board of Trustees of the Loudoun County Library, et al.

Both opponents and proponents of filtering in public institutions closely watched this case. On October 20, 1997, the Board, which manages six branches, adopted a

> "Policy on Internet Sexual Harassment" (the "Policy"), which requires that "(s)ite-blocking software ... be installed on all (library) computers" so as to: "a. block child pornography and obscene material (hard core pornography)"; and "b. block material deemed Harmful to Juveniles under applicable Virginia statutes and legal precedents (soft core pornography)." To implement the Policy, the Library Board chose "X-Stop," a commercial software product intended to limit access to sites deemed to violate the Policy. (Mainstream Loudoun, et al. . ., 1998)

It is interesting that the software was intended to deal with sexual harassment; that is, library patrons were expected to be disturbed by others viewing controversial material from the Internet, a possible form of sexual harassment. The software was installed in November and almost immediately complaints were heard (Harmon, 1998):

> The software program chosen by the county for its six library branches, X-Stop, purports to purify the Internet. But library users complain that X-Stop, produced by the Log-On Data Corp. of Anaheim, Calif., is imperfect at best. Library users complain that they have been denied access to information on sex education, breast cancer and gay and lesbian rights, among other things, because the software cannot discriminate between obscene materials and other information about sexual topics.
>
> Patrons say they have even been barred from a Quaker site on the World Wide Web and from the home page of Yale University's biology department. At the same time, they say, graphic sexual images sometimes manage to evade the software.

Not surprisingly, a group of citizens, Mainstream Loudoun, and others including the American Civil Liberties Union (ACLU) sued the Board claiming, "that the Policy impermissibly blocks their access to protected speech such as the Quaker Home Page, the Zero Population Growth website, and the site for the American Association of University Women-Maryland. . . They also claim that there are no clear criteria for blocking decisions and that defendants maintain an unblocking policy that unconstitutionally chills plaintiffs' receipt of constitutionally protected materials." (Mainstream Loudoun, et al. . ., 1998) In her decision not to render summary judgment, by dismissing the suit, District Judge Leonie M. Brinkema, made the following argument:

> To the extent that Pico applies to this case, we conclude that it stands for the proposition that the First Amendment applies to, and limits, the discretion of a public library to place content-based restrictions on access to constitutionally protected materials within its collection. Consistent with the mandate of the First Amendment, a public library, "like other enterprises operated by the State, may not be run in such a manner as to 'prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion.' " Id. at 876 (Blackmun, J., concurring) (quoting Barnette, 319 U.S. at 642).

Although recognizing the legitimate concern that public libraries have for the welfare of children, the Judge noted that, "Adult library patrons are presumed to have acquired already the 'fundamental value' needed to act as citizens, and have come to the library to pursue their personal intellectual interests rather than the curriculum of a high school classroom. As such, no curricular motive justifies a public library's decision to restrict access to Internet materials on the basis of their content." She adds the following point to reinforce her opinion: "We are therefore left with the First Amendment's central tenet that content-based restrictions on speech must be justified by a compelling governmental interest and must be narrowly tailored to achieve that end." And therefore this conclusion must follow. "Accordingly, we hold that the Library Board may not adopt and enforce content-based restrictions on access to protected Internet speech absent a compelling state interest and means narrowly drawn to achieve that end." There are other reasons for her final opinion but the foregoing represents a clear statement of the power of the First Amendment in American life.

The final decision was delivered on November 23, 1998 and given her earlier opinion, there was no surprise, as she held for the plaintiff: "Defendant will be permanently enjoined from enforcing its Policy on Internet Sexual Harassment." The Conclusion to this opinion is instructive and should serve the purpose of causing other library boards to tread carefully in restricting access to the Internet:

> Although defendant is under no obligation to provide Internet access to its patrons, it has chosen to do so and is therefore restricted by the First Amendment in the limitations it is allowed to place on patron access. Defendant has asserted a broad right to censor the expressive activity of the receipt and communication of information through the Internet with a Policy that (1) is not necessary to further any compelling government interest; (2) is not narrowly tailored; (3) restricts the access of adult patrons to protected material just because the material is unfit for minors; (4) provides inadequate standards for restricting access; and (5) provides inadequate procedural safeguards to ensure prompt judicial review. Such a Policy offends the guarantee of free speech in the First Amendment and is, therefore, unconstitutional. (Memorandum Opinion, 1998)

Even within the library community, there is considerable debate about how to balance the rights to open inquiry against parental concerns about the welfare of their children. It is possible to install filtering software on just a limited number of computers, leaving the rest unfiltered. Then parents can, if they wish, require their children to use the filtered computers. Some librarians do not find such an approach satisfactory, arguing that any restraint on access violates their professional standards. Others say that it is also unsatisfactory because patrons at unfiltered computers can be looking at images that might make those nearby uncomfortable. Recall that the Loudoun policy was ostensibly introduced to deal with sexual harassment. Other approaches include the placement of screens around unfiltered computers to provide both privacy for patrons and the concealment of possibly offensive material. Finally, there is the ubiquitous "tap on the shoulder," designed to caution patrons about excessive noise, eating or drinking, or in the present situation, the display of possibly offensive material. These approaches are also not universally accepted, clear indication of the passions aroused by filtering or any other constraints on access. For a broad overview of legal issues affecting the decisions of libraries whether or not to install filtering programs, see Internet Filtering of Libraries (2000).

Kathleen R. v. City of Livermore, et al.

On May 28, 1998, a complaint was filed against the city of Livermore, California by a plaintiff known as Kathleen B. The following summary of the complaint is taken from a brief by the city of Livermore: (Kathleen R. v. City of Livermore, et al., 1998)

> The Complaint filed by Kathleen R. ("Plaintiff") requests injunctive relief against the City of Livermore ("City") ". . . preventing it or its agents, servants, and employees from spending any public funds on the acquisition, use, and/or maintenance of any computer system connected to the Internet or World Wide Web for which it allows any person to access, display, and/or print obscene material or for which it allows minors to access, display, and/or print sexual material harmful to minors." (Complaint, pp. 5-6.) The Complaint also requests declaratory relief ". . . stating that the City of Livermore is legally liable for all future damage to plaintiff's children caused by the children accessing, acquiring, displaying, and/or printing sexual and other material harmful to minors on any library computer connected to the Internet or World Wide Web." (Id. at p.6.) These requests are based on causes of action alleging that the City is wasting public funds, creating a public nuisance and fostering potential damages claims by allowing minors to have unlimited access to the Internet.

Mendels compares this case to the one in Loudoun County and while she notes the obvious similarities, there are some striking differences: (Mendels, 1999b)

> And while the Virginia case focused on First Amendment issues, the California case could revolve around a more technical question: whether

> libraries, as a kind of Internet service provider, are shielded from certain kinds of lawsuits. . .
>
> The California case was also brought by a library patron, but there the resemblance to Loudoun ends. Kathleen R., whose last name is not disclosed in court documents, sued the city of Livermore, alleging that her 12-year-old son, Brandon P., was able to use library computers several times last year to download sexually graphic pictures, which he then copied to a disk and printed out at a relative's home.
>
> His mother's suit, filed in May, asked that taxpayer support for library computer operations be suspended as long as children had access to material deemed “harmful to minors” under California law. Her lawyer, Michael D. Millen, has suggested that the use of filters would be a good remedy.

On January 14, 1999, Judge George Hernandez dismissed the suit without issuing an opinion. Two days later, Kathleen R. appealed to the Court of Appeal of State of California. So the decision of the Livermore libraries not to install filtering software on its computers was upheld. Both Loudoun and Livermore have served as examples of an approach to the issue of accessing possibly offensive material by children, in public places, that respects a broad interpretation of the First Amendment. And in addition the ethics and professionalism of librarians has prevailed, although the assault is unrelenting.

Current Legal Positions

First Amendment protection is the basic defense for free speech in the U.S. and any proposed laws that are directed towards limiting access to the Internet must demonstrate that sufficient reason exists to restrict the application of the First Amendment. Precedent exists in obscenity laws, child pornography laws, threats, and libel. Thus the absolutist language of the First Amendment has been compromised on many occasions because of competing societal interests. No further constitutional analysis will be attempted here other than to comment on the degree to which children have First Amendment rights, a relevant issue given that children will be most affected by the deployment of filtering software in schools and libraries. Of course, parents have the freedom to act as they wish in their own homes. As Carl Kaplan asks in his column on legal issues in the *New York Times*, (Kaplan, 1998): “Do children have a First Amendment right to obtain indecent materials?” There is no clear answer offered in the article.

One constitutional scholar “believes children have diminished rights to indecent material.” He goes on to say,

> “It's a nice question [whether children have a right to indecent material], and the general answer would appear to be ‘no’ William W. Van Alstyne, a professor at Duke University School of Law and the author of a leading textbook on the First Amendment, said in a recent wide-ranging telephone

> interview. He defined indecent speech as ‘sexually graphic or explicit’ material that is ‘offensive to ordinary sensibilities.’ Unlike obscenity, such material may have redeeming social value.
>
> ‘Children don't have the same First Amendment rights adults, though they do have some First Amendment rights,’ Van Alstyne explained. Children's speech rights ‘are diminished in direct proportion to youth -- the younger the child, the greater degree of permissible regulation of what they may have access to,’ he said.” (Kaplan, 1998)

The contrary position is offered by Chris Hansen, a senior lawyer with the ACLU, who, “thinks that children have strong rights to obtain valuable material, such as AIDS information and art of nudes - even if it might be sexually explicit and offensive to some people.” And he reiterates the traditional argument against filters, “that all filtering programs inadvertently block material that is not indecent and constitutionally protected. 'So if you force kids onto machines that filtered, the odds are high that you will be depriving them of access to information that everybody would agree they should see’.”

In terms of other civil rights, the courts have generally supported the right of school officials to carry out searches of student lockers for drugs and weapons without obtaining search warrants. It will be difficult therefore, if not impossible, to resist the widespread implementation of filtering software. The opposition to the implementation of such software was originally supported by civil liberties groups, as well as computer and software manufacturers, ISPs, and information providers as they sought to prevent the Computer Decency Act (CDA), a section of the Telecommunications Act of 1996 from taking effect. In this context of opposing the CDA, these groups and companies successfully argued that the intentions of Congress could be carried out by employing filtering software, a technology seemingly growing in sophistication and effectiveness. The crucial section of the CDA defines the issues of concern.[4] A three-judge panel in Philadelphia voiced a strong defense of free speech in their opinion: (ACLU v. Reno, 1996)

[4] **TITLE V - Communications Decency Act of 1996, Section 502, Obscene or Harassing Use of Telecommunications Facilities.**

(a) Whoever--
(1) in interstate or foreign communications--
(A) by means of a telecommunications device knowingly--
(i) makes, creates, or solicits, and
(ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person;
(B) by means of a telecommunications device knowingly--
(i) makes, creates, or solicits, and
(ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

- The Internet may fairly be regarded as a never-ending worldwide conversation. The government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from government intrusion. . .
- Any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig.
- Internet communication, while unique, is more akin to telephone communication than to broadcasting because as with the telephone an Internet user must act affirmatively and deliberately to retrieve specific information online.
- Just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects.
- The CDA will, without doubt, undermine the substantive, speech-enhancing benefits that have flowed from the Internet. The diversity of the content will necessarily diminish as a result. The economic costs associated with compliance with the Act will drive from the Internet speakers whose content falls within the zone of possible prosecution.

The judges were impressed by the performance of such filtering software as CyberSitter, SurfWatch, and NetNanny. As these programs seem to have become more effective, their use has become the focus of concern.

Proposed Legislation

COPA (Child Online Protection Act of 1998)

The fact that the Supreme Court upheld the lower court decision declaring certain sections of the CDA unconstitutional in June 1997 did not end the attempts of Congress to address the issue of shielding children, not only from sexually explicit material but from excessive violence and hate and racism as well. Thus, on October 21, 1998, President Clinton signed into law the Omnibus Appropriations Act of 1998 that included the Child Online Protection Act, subsequently dubbed CDA II, or child of CDA. Given that sections of CDA were found unconstitutional, one might have

(C) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications;

(D) makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number; or

(E) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication; or

(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18, United States Code, or imprisoned not more than two years, or both.';

expected that this attempt to ensure the constitutionality of COPA would have been better founded. But there were some obvious problems, namely, the following: (Constitutional Analysis of the Oxley Bill, 1998)

1. Imposes serious burdens on constitutionally-protected speech, including materials such as the recently released Starr report, movies, and television programs, when disseminated through popular commercial Web sites such as CNN, Yahoo, or MS-NBC.
2. Fails to effectively serve the government's interest in protecting children, since it will not effectively prevent children from seeing inappropriate material originating from outside of the U.S. nor will it cover material available through other Internet resources besides the World Wide Web, such as chat rooms or email.
3. Does not represent the least restrictive means of regulating speech, according to the Supreme Court's findings that blocking and filtering software give parents the ability to screen out undesirable content without burdening speech. Congress has not produced an adequate record to refute this finding or to support the notion that H.R. 3783 is the least restrictive means of protecting children.

On October 22, 1998, the ACLU et. al. filed a motion for a temporary restraining order against this bill. Among other things, the memorandum pointed out that before COPA had been enacted, the Department of Justice had written, "a seven-page letter to Congress outlining 'serious concerns' about the bill, and warning that it 'would likely be challenged on constitutional grounds'." (American Civil Liberties Union, et. al. v. Janet Reno, 1998) Given that COPA represents a second attempt to control access, it is surprising that serious constitutional problems remain. For example, in commenting on the requirements to verify age effectively, the memorandum notes,

> Even if age or credit card verification were feasible, such a requirement would fundamentally alter the nature and values of the new computer communication medium, which is characterized by spontaneous, instantaneous, albeit often unpredictable, communication by hundreds of thousands of individual speakers around the globe, and which provides an affordable and often seamless means of accessing an enormous and diverse body of information, ideas and viewpoints.
>
> The COPA would thus prevent or deter hundreds of thousands of readers from accessing protected speech even if it were feasible for speakers to set up a system to verify age. Any age verification requirement would inevitably prevent readers who lack the necessary identification from accessing speech that would otherwise be available to them. Many adults do not have a credit card. Age verification would have an especially detrimental effect on foreign users, who are less likely than U.S.-based adults to have a credit card or other identification.

On February 1, 1999, Judge Lowell A. Reed Jr. of United States District Court in Philadelphia found in favour of the plaintiffs and issued a preliminary injunction, blocking the enactment of COPA. The conclusion to Judge Reed's opinion[5] is revealing in its expression of the dilemma for those who believe that children must be legally protected against certain kinds of material on the Internet, while at the same time not depriving adults of their free speech rights. More narrowly focused efforts have been undertaken over the last two years in Congress, although none have yet been enacted.

Current Filtering Bills

Several specific bills have been introduced, but none yet passed, to require schools, libraries, and other groups that receive federal financial support to connect their computers to the Internet, to install filtering software on those computers. Since children would be the sole users of these computers, especially in the schools, the expectation is that constitutional concerns would be considerably lessened. Some examples of these attempts will be briefly reviewed.

On January 19, 1999, Senator John McCain introduced S 97, the Children's Internet Protection Act, approved by the Commerce Committee on June 23. The key

[5] **Conclusion to Judge Reed's Opinion in ACLU et. al. v. Janet Reno, In the United States District Court for the Eastern District of Pennsylvania, February 1, 1999**

The protection of children from access to harmful to minors materials on the Web, the compelling interest sought to be furthered by Congress in COPA, particularly resonates with the Court. This Court and many parents and grandparents would like to see the efforts of Congress to protect children from harmful materials on the Internet to ultimately succeed and the will of the majority of citizens in this country to be realized through the enforcement of an act of Congress. However, the Court is acutely cognizant of its charge under the law of this country not to protect the majoritarian will at the expense of stifling the rights embodied in the Constitution. Even at this preliminary stage of the case, I borrow from Justice Kennedy, who faced a similar dilemma when the Supreme Court struck down a statute that criminalized the burning of the American flag:

The case before us illustrates better than most that the judicial power is often difficult in its exercise. We cannot here ask another Branch to share responsibility, as when the argument is made that a statute is flawed or incomplete. For we are presented with a clear and simple statute to be judged against a pure command of the Constitution. The outcome can be laid at no door but ours.

The hard fact is that sometimes we must make decisions that we do not like. We make them because they are right, right in the sense that the law and the Constitution, as we see them, compel the result. And so great is our commitment to the process that, except in the rare case, we do not pause to

The hard fact is that sometimes we must make decisions that we do not like. We make them because they are right, right in the sense that the law and the Constitution, as we see them, compel the result. And so great is our commitment to the process that, except in the rare case, we do not pause to express distaste for the result, perhaps for fear of undermining a valued principle that dictates the decision. This is one of those rare cases.

Texas v. Johnson, 491 U.S. 397, 420 (1989) (Kennedy, J., concurring).

. . .

Based on the foregoing analysis, the motion to dismiss the plaintiffs for a lack of standing will be denied. Based on the foregoing findings and analysis, the Court concludes that the plaintiffs have established a likelihood of success on the merits, irreparable harm, and that the balance of interests, including the interest of the public, weighs in favor of enjoining the enforcement of this statute pending a trial on the merits, and the motion of plaintiffs for a preliminary injunction will be granted.

elements are given as follows: (Summary of Filtering Bills in the 106th Congress, 1999)

> "an elementary or secondary school computers with Internet access may not receive services at discount rates ... unless ... (it) (i) has selected a technology for its computers with Internet access in order to filter or block Internet access through such computers to (I) material that is obscene; and (II) child pornography; and (ii) is enforcing a policy to ensure the operation of the technology during any use of such computers by minors."

The House passed a similar bill but so far no further action has been taken. The McCain bill is applicable only to schools that benefit from the E-rate, a discount rate for connecting to the Internet. In the House, the Child Protection Act was introduced on July 20, 1999. It will apply to all schools and libraries that use Federal funds to acquire or operate computers and requires them to,

> "(1) install software on that computer that is determined ... to be adequately designed to prevent minors from obtaining access to any obscene information or child pornography using that computer; and (2) ensure that such software is operational whenever that computer is used by minors, ..."

Regulating Violence

1999 seems noteworthy for a sequence of acts involving deadly violence against innocent victims in school (Littleton, Colorado), in church (Fort Worth), in a day care (Los Angeles), and on the streets (Illinois). Children were often the targets or the perpetrators and so it was not surprising that violence and hate soon become the primary targets of those who wished to regulate the Internet. In fact shortly after the tragic events in Littleton Colorado, Vice-President Gore, in response to reported steps taken by filtering companies to improve the effectiveness of their software to restrict access to hate sites, hailed these effort because they would "honor the lives" of the victims. (Gore Says Internet Limits ..., 1999) He also said in the interview. "Where the Internet is concerned, this will give parents more tools to employ the latest blocking and filtering technologies to limit access to sites that are run by hate groups, violent games and other materials." But of course these tools will certainly be employed in schools and libraries and the exercise of open access will be compromised.

Within a month, Representative Henry Hyde of Illinois introduced the Protecting Children from the Culture of Violence Act as an amendment to the Juvenile Justice Act. Although the Internet is not explicitly mentioned, this bill certainly would apply as it, "would prohibit the sale to minors of any image content that contains sexually explicit or violent material." (Macavinta, 1999) If passed, this bill would extend the limitations on accessing Web content beyond sexual explicitness to violence and hate. Note the following, taken from the proposed Act:

> Overall, the amendment makes it illegal to sell those under age of 17 “any picture, photograph, drawing, sculpture, video game, motion picture film, or similar visual representation or image, book, pamphlet, magazine, printed matter, or sound recording” that an average person would find “patently offensive with the respect to what is suitable for minors.” The material would have to lack serious literary, artistic, political, or scientific value.

In spite of the fact that there appears to be little evidence that the Internet is a contributing factor to the kinds of violence referred to above, it has become the cause of choice. Surely, parents must be concerned about many issues in raising their children, the Internet being one but not perhaps the most serious. For more on this topic, a recent report issued by the Senate Judiciary Committee is quite instructive. (Children, Violence, and the Media, 1999) in that it does argue for a direct connection between violence in the media, including the Internet, and violence in real life and suggests that federal measures are necessary in order to ensure that the use of increasingly effective filtering programs is mandated.

SUMMARY AND CONCLUSIONS

There appear to be many reasons for the general public to be concerned about the Internet. Media pieces abound of sex, nudity, child pornography, child seductions, violence, bomb-making instructions, and even more, readily available on the Internet. But as (Turow, 1999) points out very clearly, media reports on the Internet have been very narrowly focused; so articles reporting some instance certain to alarm parents, rarely place it in perspective. That is, the impression is left that the Internet is rife with possibly detrimental material and that events of the sort being reported are the rule not the exception. The repercussions of such impressions are compounded by the occurrence of serious acts of violence, with some regularity in the U.S., that are also linked to the apparent availability of violent and hateful material on the Internet, to say nothing of the ready availability of guns of all sizes.

Another strand in the story developed in this paper is the obvious motivation of large international Internet companies to make the Internet a safe place to do business. E-commerce has been hailed as the engine of growth for the world's advanced economies. However, a necessary precondition to the growth of E-commerce is to establish that the world of the Internet is equivalent to that of the existing situation of personal shopping. This effort is massive and ongoing and certainly is a driving force behind attempts to mandate the regulation of the Internet whether by means of filtering software controlled by parents at home or mandated in public libraries and schools by the government. And this effort is ongoing and growing as large companies combine to propose ever more sophisticated rating systems. Witness the recent efforts of the Bertelsmann Foundation (Self-regulation of Internet Content, 1999) to rally support for an international rating system for self-regulation of the Internet.

Finally, our story would be incomplete without the role played by civil liberties and consumer groups in arguing against the constitutionality of the Communications

Decency Act of 1996. Judges in various courts were persuaded that parents could avail themselves of filtering software to control what they felt was harmful for their children in contrast to the dangers of violating the First Amendment by Federal government actions. This part is more or less uncontroversial, even though parents might be misled into believing that filtering software is more precise than it actually is. At worse, useful sites may be blocked on home computers and therefore valuable information made unavailable. It is the public use of such software that has become the concern as exemplified in several filtering bills before Congress. In addition, the battle for free speech must be fought at almost every public library and school.

The global initiative to regulate the Internet on a voluntary basis is obviously in full swing. As has been suggested earlier, self-rating systems have their own dangers, particularly the creation of a sanitized product that bears little relation to the world, as we know it. Presumably, each country will select only certain scales to rate sites or will vary in the settings of relevant scales. The burden on Web sites will be excessive and it will be straightforward to banish certain of them to an outlaw section of cyberspace. Of course, inventive children will be sorely tempted to explore just that part of the Internet, where they are not supposed to go, and may well succeed in their endeavours. But the situation may be even worse than this as controversial Web sites create mirror sites, whose URL's are circulated by e-mail among interested parties, including children, as described by Paquin, (1999).

The drive to regulate, control, and limit or deny access to information is ever present. Consider this observation, taken from (PFIR Statement on Content Control and Ratings, 2000) about singling out the Internet for special treatment:

> It is particularly alarming to observe the extent to which the proponents of mandatory filtering seem anxious to control Internet content that is not similarly controlled in other situations. A common example frequently cited is information about explosives. There is certainly such information available on the Internet, which could be used to harm both persons and property. But much of this same sort of information is available in bookstores, libraries, or by mail order. How do we draw the line on what would be forbidden? Radical literature? Industrial training materials? Chemistry textbooks? Are we really so anxious to dramatically alter our notions of free speech across the board, not just relating to the Internet?

The reasons to limit access may vary over time and place from the protection of children to society in general. The relatively new Internet has become the current battleground in this long-standing conflict. It remains for those, who value free speech and open inquiry and debate, to join this battle and defend these freedoms for present and future generations. As Judge Reed notes in his decision, (Reed. 1999)

> Despite the Court's personal regret that this preliminary injunction will delay once again the careful protection of our children, I without hesitation acknowledge the duty imposed on the Court and the greater good such duty serves. Indeed, perhaps we do the minors of this country harm if First

Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection.

Acknowledgments

The support of the Natural Science and Engineering Research Council is gratefully acknowledged. Thanks are also extended to David Jones and Jeff Shallit of Electronic Frontier Canada, to the many students who challenged my views, and to the anonymous reviewers who offered their constructive criticisms. Finally, let me acknowledge my appreciation to my wife, Sheryl Adam, a librarian at the University of British Columbia, and to all librarians for their defense of free and open inquiry.

References

ACLU v. Reno (1996) Full Text of Opinion, June 12. Accessed from the Web site with URL: http://www.epic.org on June 13, 1996.

American Civil Liberties Union, et. al. v. Janet Reno (1998) Plaintiffs' Memorandum of law on Support of Their Motion for a Temporary Restraining Order and Preliminary Injunction, September 22. Accessed from the Web page with URL: http://www.aclu.org/court/acluvrenoII_tro.html on November 20, 1998.

American Civil Liberties Union, et. al. v. Janet Reno (1999) Judge Reed's Opinion in the United States District Court for the Eastern District of Pennsylvania, February 1. Accessed from the Web page with URL: http://www.paed.uscourts.gov/opinions/99D0078P.HTM on August 23, 1999.

American Library Association (1997) Statement on Library Use of Filtering Software. Accessed from the Web site with URL: http://www.ala.org/alaorg/oif/filt_stm.html on June 15, 1998.

Censorship's Tools Du Jour: V-Chips, TV Ratings, PICS, and Internet Filters (1998) The National Coalition Against Censorship, March. Accessed from the Web page with URL: http://www.ncac.org/toolsdujour.html on June 15, 1998.

Children, Violence, and the Media (1999) Senate Committee on the Judiciary, September 14. Accessed from the Web page with URL: http://www.senate.gov/~judiciary/mediavio.htm on September 23, 1999

Code of the Comic Magazine Association of America (1971) Accessed from the Web site with URL: http://www.mit.edu/activities/safe/labeling/comics-code-1971 on September 6, 1999.

Constitutional Analysis of the Oxley Bill (1998) Center for Democracy and Technology. Accessed from the Web Page with URL: http://www.cdt.org/speech/constitutional.html on October 9, 1998.

Gore Says Internet Limits 'Honor the Lives" of School Victims (1999) Associated Press, May 5. Accessed from the Web page with URL: http://www.nytimes.com/library/tech/99/05/biztech/articles/05gore.html on May 11.

Harmon, A. (1998) Virginia Library Lawsuit Seen as Litmus Test for Internet Freedom, *New York Times*, March 2. Accessed from the Web page with URL:

http://www.nytimes.com/library/tech/98/03/biztech/articles/02library.html on July 30, 1998.

Hochheiser, H. (1998) Filtering FAQ, Computer Professionals for Social Responsibility, Version 1.1.1. Accessed from the Web site with URL: http://www.cpsr.org/filters/faq.htm on September 6, 1999.

Internet Filtering of Libraries (2000) A memorandum from Jenner & Block to the American Library Association. Accessed from the Web Site with URL: http://www.ftrf.org/internetfilteringmemo.html on May 20, 2000.

June 1999 Web Statistics (1999) Online Computer Library Center, September 9. Accessed from the Web page with URL: http://www.oclc.org/oclc/press/19990908a.htm on September 20, 1999.

Kaplan, C. S. (1998) Children's First Amendment Rights Lost in the Filtering Debate, *New York Times*, March 6. Accessed from the Web page with URL: http://www.nytimes.com/library/tech/98/03/cyber/cyberlaw/06law.html on July 30, 1998.

Kathleen R. v. City of Livermore, et al. (1998) In the Superior Court of the State of California in and for the County of Alameda, October 21. Accessed from the Web page with URL: http://www.techlawjournal.com/courts/kathleenr/80710livbr.htm on December 4, 1998.

Kids Online (1999) NFO Interactive. Accessed from the e-marketer Web page with URL: http://www.emarketer.com/estats/061499_kids.html on June 15, 1999.

Lawrence, S. and Giles, C. L. (1999) Accessibility of Information on the Web, *Nature*, **400**, July 8, 107-109. Accessed from the Web site with URL: http://www.nature.com on July 31, 1999.

Lazarus, D. (1999) Firm Says Kids Visit Questionable Web Sites at School, *San Francisco Chronicle*, September 6. Accessed from the Web page with URL: http://www.websense.com/news/sf090699.htm on September 10, 1999. A PowerPoint presentation of these findings is available at http://www.websense.com/news/ppt/ystudy.ppt.

Lessig, L. (1998) What Things Regulate Speech: CDA 2.0 vs. Filtering, Draft 3.01, May 12. Accessed from the Web page with URL: http://cyber.harvard.edu/works/lessig/what_things.pdf on February 1, 1999.

Macavinta, C. (1999) Bill Limits Children's Exposure to Violence*,* *CNet News*, June 11. Accessed from the Web page with URL: http://www.news.com/News/Item/0,4,37727,00.html?st.ne.fd.gif.d on June 11, 1999.

Mainstream Loudoun, et al. v. Board of Trustees of the Loudoun Country Library, et al. (1998) United States District Court for the Eastern District of Virginia, April 7. Accessed from the Web page with URL: http://www.venable.com/ORACLE/opinion.htm on October 2, 1998.

Memorandum Opinion (1998) Re: Mainstream Loudoun v. Loudoun County Library. U.S. District Court, Eastern District of Virginia, Case No. 97-2049-A. Date: November 23, 1998. Accessed from the Web page with URL:

http://www.techlawjournal.com/courts/loudon/81123op.htm on November 24, 1998.

Mendels, P. (1999a) Survey Indicates Increased Use of Filters, *New York Times*, May 12. Accessed from the Web page with URL: http://www.nytimes.com/library/tech/99/05/cyber/education/12education.html on May 11, 1999.

Mendels, P. (1999b) Court Tackles New Angle on Library Internet Filtering, *New York Times*, December 4. Accessed from the Web page with URL: http://www.nytimes.com/library/tech/98/12/cyber/cyberlaw/04law.html on December 4, 1998.

Paquin, R. (1999) Why filters will be less "technically" effective as time goes on. Posted on the American Library Association Office of Intellectual Freedom (ALAOIF) Listserv on October 1, 1999.

Pending Bills Would Impact Online Speech. (2000) Epic Alert, **7.08**,.Accessed from the Web Site with URL: http://www.epic.org/alert/EPIC_Alert_7.08.html

PFIR Statement on Control and Ratings (2000) People for Internet Responsibility. Accessed from the Web site with URL: http://www.pfir.org/statements/2000-03-18

Reed Jr., L. A. (1999) In the United States District Court for the Eastern District of Pennsylvania, Civil Action, American Civil Liberties Union et al. v. Janet Reno, No. 98-5591, February 1. Accessed from the Web site with URL: http://www.paed.uscourts.gov/opinions/99D0078P.HTM on August 23, 1999.

Resnick, P. (1997) Filtering Information on the Internet, *Scientific American*, March. Accessed from The Web site with URL: http://www.sciam.com/0397issue/0397resnick.html on March 6, 1998. See also Hochheiser, H. (1998).

Rosenberg, R.. S. (1999) Filtering the Internet in the USA: Free Speech Denied? *The Fourth ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communication Technologies*, October 6-8, Rome, Italy.

Self-regulation of Internet Content (1999) Bertelsmann Foundation. Accessed from the Web page with URL: http://www.stiftung.bertelsmann.de/internetcontent/english/download/Memorandum.pdf on September 10, 1999.

Summary of Filtering Bills in the 106th Congress (1999) *Tech Law Journal*, August 15. Accessed from the Web page with URL: http://www.techlawjournal.com/cong106/filter/Default.htm on September 20, 1999.

Turow, J. (1999) The Internet and the Family: The View from Parents, The View from the Press, The Annenberg Public Policy Center of the University of Pennsylvania.. Accessed from the Web page with URL: http://www.appcpenn.org/appc/reports/rep27.pdf on May 6, 1999.

Turow, J. and Nir, L. (2000) The Internet and the Family 2000: The View from Parents, The View from Kids, The Annenberg Public Policy Center of the

University of Pennsylvania. Accessed from the Web page with URL: http://appcpenn.org/finalrepor_fam.pdf on May 20, 2000.

Weinberg, J. (1997) Rating the Net, 19 *Hastings Comm/Ent L.J.* 453. Accessed from the Web page with URL: http://www.msen.com/~weinberg/rating.htm on March 6, 1998.

Biography

Richard S. Rosenberg is a Professor in the Department of Computer Science, at the University of British Columbia. His research interests are in Artificial Intelligence (AI) and the social impact of computers. In AI, he has published in computational linguistics, with a special interest in natural language interfaces to databases and the Web. His work in the social impact of computers includes such areas of concern as privacy, freedom of expression, intellectual property rights, universal access, work and education. His, most recent book is *The Social Impact of Computers*, 2nd Edition, San Diego, CA: Academic Press, 1997. He is vice-president of Electric Frontier Canada.