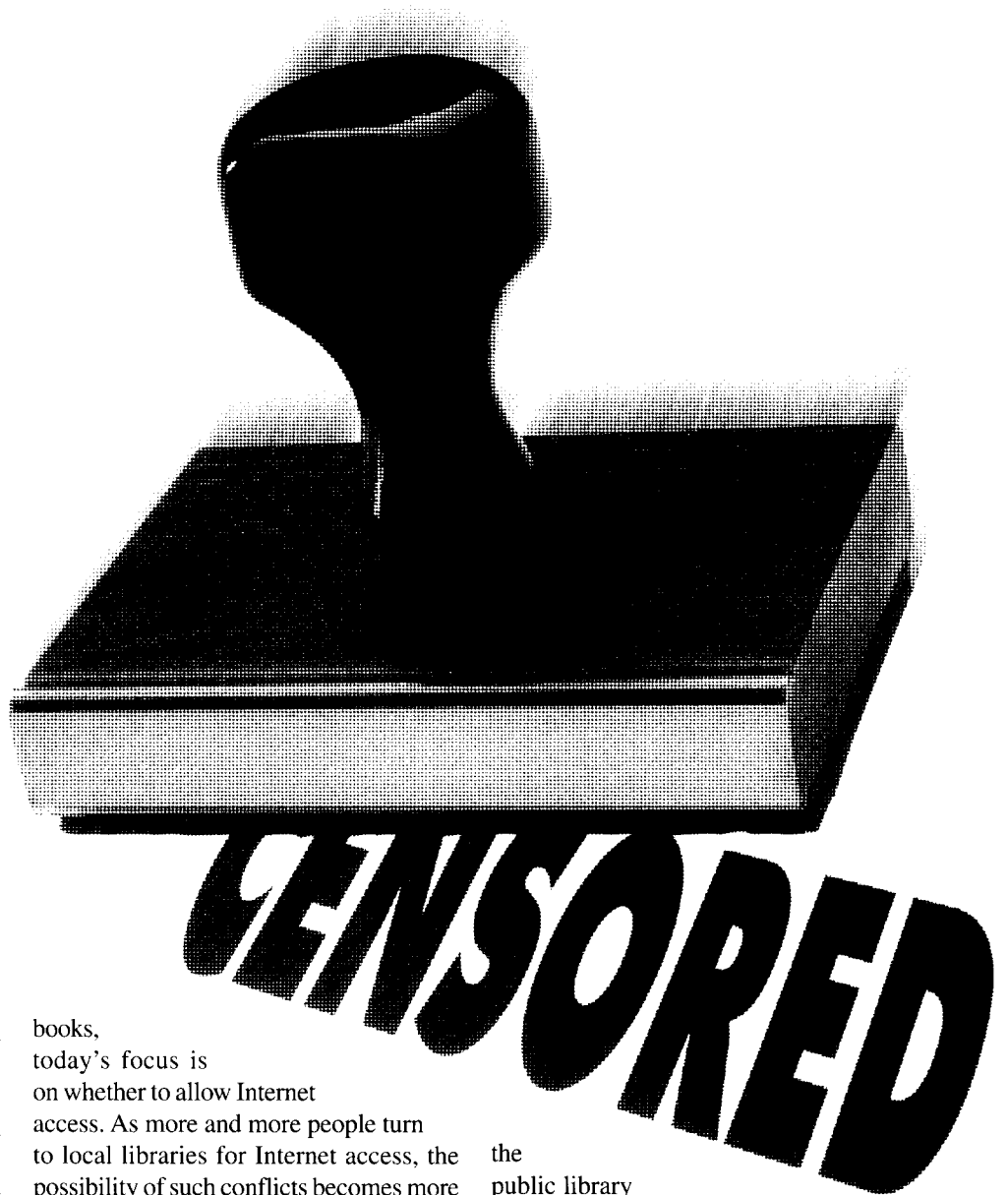


# Filtering the Net in Libraries: The Case (Mostly) in Favor

by Michael A. Banks

*Filters are tools  
that help librarians  
keep inappropriate  
material out of  
their libraries.*



The year is 1967. A patron finds a book in your library containing detailed instructions for making dynamite, and uses that information to build a bomb that he uses to destroy a neighbor's house. Now, you are being sued—and you may be charged with complicity in a crime.

Or, it's 1972, and last month you refused to allow a young patron to withdraw books from the "adult" section of your library. Despite the long-standing rule that anyone under 12 is restricted to the juvenile and reference sections, a lawsuit is brought, naming you, library staff, and trustees as defendants.

Absurd? Unthinkable? Indeed, yes—in those times. But such scenarios are possible now, with one major difference. Rather than allowing access to the "wrong" sort of books, or denying access to certain

books, today's focus is on whether to allow Internet access. As more and more people turn to local libraries for Internet access, the possibility of such conflicts becomes more probable. This situation has forced more than a few libraries to pass judgment on what Internet content is appropriate for adults and children to see. The task is simple in theory, but complex in practice. Exactly what should you permit, and what should you block? And why?

At the same time, some communities and/or individuals are demanding that libraries abstain from such judgment. For example, late in December 1997 a community group in Virginia filed suit against

the public library system in Louden County in order to block an Internet usage policy. Among other things, the policy specified that library computers used for Internet access be equipped with filtering software, to protect children from pornography and other objectionable material on the Web and in Usenet newsgroups. The lawsuit claims that the use of such software is a violation of free speech rights, since material that adults may want to access is also blocked.

In short, even though you are not expected to have on hand every magazine and every book in the world, you are expected by many to provide access to the full Internet. Since, as the Virginia case proves, there are no hard and fast definitions of what constitutes community standards, the judgment calls are difficult, to say the least. Then there are the widely varying expectations of patrons as to their rights in using library equipment—often quite independent of any perceived community standards. All of this leaves some librarians trying to answer the question: Do you prefer to be liable for “infringing” on freedom of speech, or do you prefer to be liable for the effects of exposure to objectionable text and images?

### *To Block, or Not to Block?*

The decision to apply blocks is an unfortunate situation, indeed, but one that many libraries will have to face over the next few years. With fewer than 40 percent of American households on the Internet, more and more people are turning to libraries for Internet access. Even patrons who have Internet access at home also use library computers to get online, a matter of convenience during library visits. This means that, sooner or later, someone is going to have a problem with what they or others can or cannot access on the Internet. So, what do you do? Allow everyone access to everything, or try to control what is available?

On the whole, I feel that it is simpler to opt for blocking or filtering Internet access. That way, you don't risk offending employees and patrons who don't want to see objectionable material. This is to say, the “liability” is less than if you permit wide-open Internet access because once that genie is out of the bottle, there is no turning back. If there are objections to blocking in your community, they can be sorted out and problems rectified (not the case if you don't block and minors are accessing Internet pornography through your system). The only questions that remain are what you filter out, and how.

### *No Newsgroups Is Good Newsgroups?*

For those concerned about Internet security, I advise blocking all Usenet news-

group access. Usenet newsgroups, in existence since 1979, are one of the oldest components of the Internet. Today, this venerable element is fast becoming all

## ***“I see filters as part of a complete Internet security program.”***

but useless. Why? Because nearly all of the 20,000-plus newsgroups are clogged and choked with “spam,” mass advertising of useless moneymaking schemes, con games, and porno sites. In some newsgroups, it is impossible to sort out the worthwhile postings from the spam, thanks to the perpetrators' attempts to disguise the true nature of their postings. Also, many postings are literal traps and ambushes. As I'll show you below, the simple act of opening a newsgroup posting can cause your browser to be taken over completely. Certain Web pages can do the same thing but, fortunately, there are ways to defend against this happening—but only if you use Netscape.

This is why you might be wise to block all Usenet newsgroup access. Simply not installing the newsgroup reader element of your Web browser will do the trick. Or, you can rely on filtering software that blocks objectionable newsgroups. Remember, though, that almost any newsgroup can contain objectionable material—or the ambushes to which I referred above.

### *What About Filters?*

I see filters as part of a complete Internet security program. There are a dozen or more good Web/newsgroup filters available, each as good as the next in certain respects. There's not enough room to cover all of them here, but I will provide an overview of a few of the better products. Before I do that, though, let's take a quick look at what filtering programs do.

Acting as a Web browser “supervisor,” a filtering program prevents access to sites considered inappropriate for the person using the browser. The decision as to what is inappropriate is usually based on

listings compiled by the software manufacturer or by one of the Internet rating services. (Some companies also accept recommendations from users for sites to be blocked or unblocked.) Most programs block “adult” or sexual material, as well as sites with racist or bigotry-oriented themes. Sites promoting drug abuse are also blocked, along with adult online chat rooms. Various criteria are used to select sites to block, including the use of keywords, selective filtering of domains, and manual selection.

Unfortunately, filtering programs can be quite literal. At least one will not let you access a site or page carrying the surname or title “Sexton,” because the word “sex” is contained in that name. However, if the software allows you to unblock sites manually, this problem can be overcome easily enough. With that in mind, you will want to ask yourself these questions when selecting a filtering program:

- Is the program updatable? Most filtering programs provide online updates of blocked site lists, sometimes by subscription. Relying on such updates is a good idea, as thousands of new potentially objectionable sites come online each month. The publishers that provide updates can catch almost all of these, and they do all the work for you.
- Can I unblock selected sites? Sometimes a filtering program mistakenly blocks a site that is not offensive. When this is the case, you should be able to unblock that site.
- Can I block selected sites? Despite all their efforts, the companies that publish blocking software cannot catch every objectionable site. Thus, you will want to be able to add sites to the blocked list.

In addition to altering lists of blocked sites, you may want to be able to alter the criteria that a filtering program uses to block sites on its own. This allows you to make up your own rules as to what is blocked, and why. The more versatility in this area, the better.

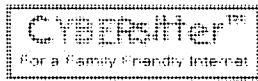
The following programs are among the better ones available. Since most blocking programs feature explanations of their blocking criteria at their Web sites, and some provide lists of blocked sites, I urge you to visit the Web site for each.

**Cyber Patrol:** Cyber Patrol is among the more successful Web filtering programs. It is used by America Online, AT&T



WorldNet, Bell Atlantic, British Telecom, and CompuServe, among other online services and Internet service providers (ISPs), and it is bundled with some PCs. You can set up Cyber Patrol to control access to the Internet and newsgroups based on a variety of criteria. Or, you can grant access only to Cyber Patrol's list of approved sites (some 40,000) and block the rest of the Web. A particularly interesting feature of the program is an option that blocks users from typing in or viewing objectionable words or phrases, based in part on a default list of profanity. A special subscription service provides online updates to Cyber Patrol's blocked site lists. For more information, and to download a free trial version, visit <http://www.cyberpatrol.com>.

**CYBERSitter:** CYBERSitter is an interesting filtering/blocking program that runs in the background at all times and claims to be virtually impossible to de-

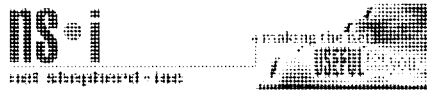


fect or defeat. It works on several fronts. By default, it not only blocks access to adult-oriented Web sites, but also to newsgroups and images. In addition, Web pages and newsgroup postings are filtered to remove offensive language. Blocking and filtering are based on lists provided with the program, but you can add you own words to the lists. When filtering, CYBERSitter examines words and phrases in context, in order to eliminate some of the ambiguity of blocking. For more information about CYBERSitter, or to download a free trial version of the program, visit <http://www.solidoak.com>.

**NetNanny:** NetNanny is designed to manage Internet and computer access. You can use it to monitor, screen, or block access to anything that is on or running into, out of, or through a computer, online or off. The outgoing block can be useful in preventing users from using search engines to find and link to objectionable sites.

The program comes with a list of blocked Internet sites and other parameters that it uses to block still more sites. The list and parameters can be updated at no charge at the NetNanny Web site, and you can add your own screening specifications. NetNanny is available for Windows or DOS. See <http://www.netnanny.com> for more information.

**Net Shepherd:** Net Shepherd is an Internet content rating service that filters the results of AltaVista searches. Its PICS-compliant ratings database can be used



with Microsoft Internet Explorer or Net Shepherd's own daxHOUND program, a content filtering tool. For additional information on Net Shepherd, visit <http://www.netshepherd.com>. Information about daxHOUND (and a download) can be found at <http://www.netshepherd.com/products/daxHOUND2.0/daxhound.htm>.

**SurfWatch:** SurfWatch is a filter that screens for unwanted material on the Internet. As with other filter and blocking programs, SurfWatch can be used with almost any Web browser. Various levels of access control are available, and the program cannot be easily disarmed by deleting it or by other means. SurfWatch

***"It is easy to see the absurdity of uncontrolled Internet access for children and other patrons."***

screens Web sites, newsgroups, ftp and gopher sites, and Web chat rooms. Blocking is based on a list of sites generated by in-house research and customer reports. Online updates are available via subscription.

SurfWatch alone doesn't permit you to modify the list of sites, nor does it attempt to block sites that are violent in nature or include material that is hateful or

otherwise potentially inappropriate. A free add-on called SurfWatch Manager lets you edit the list of blocked sites. Full information on SurfWatch, along with its list of blocked sites, is available at <http://www.surfwatch.com>.

**X-STOP:** The appropriately named X-STOP is a program designed for use by libraries and other institutions and businesses that provide Internet access. It selectively blocks and filters sites based on a variety of criteria. The program allows you to alter the criteria it uses for filtering. It also monitors outgoing words in order to prevent users from looking up objectionable sites with search engines. For more information, see <http://www.xstop.com>.

### *Ambushed by Java and JavaScript Risks*

Even if you use a filtering program with your computer systems, you can still run into security problems, thanks to Java and JavaScript. You are probably aware of the many security risks associated with Java, a programming language that is used to transmit small computer programs, called "applets" to Internet users' computers, where they are free to run and do things like collect data from hard drives. Filtering programs cannot detect everything a Java program will do, so it is possible to transmit objectionable content with a Java applet. Thus, it is usually a good idea to disable Java on your browsers. It is true that Java-related risks are fewer since so many "loopholes" involving Java have been exposed. But you never know what someone is cooking up. Besides, the Java-less Web surfer usually misses nothing more than animations that slow down browsing anyway.

JavaScript can pose a slightly greater risk, for two reasons. First, there have been no warnings about problems created by JavaScript. Indeed, I expect this to be the first you've heard of such problems. JavaScript can be used to direct your browser to any page on the Web, alter its configuration, and pull other nasty tricks. This being the case, it is best to disable JavaScript when visiting Web sites unfamiliar to you, and when reading newsgroup messages, in which JavaScript can be used to take over browsers.

Second, the JavaScript language is far easier to use, and thus accessible to more

people, than Java. This means that the risk of exposure to malevolent JavaScript code is greater. What can JavaScript do to your system? For openers, JavaScript can be used to take control of a browser from a Web page or a Usenet newsgroup posting in two different ways. With a simple line of code, someone can set up a page so that, should your mouse cursor pass over a link or an image (loaded or not), your browser will be forced to “go to” (load) a specified page on the Web. This happens without clicking on anything.

A more insidious JavaScript trick can take over your browser and re-open it without menus or controls, on top of all other applications. Here again, the perpetrator of this trick can put anything he or she wants to appear in your browser window. This not only forces you to look at the perpetrator’s message or images, but also disrupts your browsing session. And it can get worse. I have seen this set up so that you are forced to see the same page—or a series of pages—over and over again. Even if you exit the browser, it will re-open and display whatever the perpetrator wants it to display. This has been used extensively by pornography site purveyors to force Web surfers to their sites and to keep them there. Worse, the code required to do the things just described can be hidden, so that you cannot see it even if you view a Web page’s source.

The only defense against this is to disable JavaScript. This is easily done with Netscape. Unfortunately, you cannot disable JavaScript if you are using Microsoft Internet Explorer 4. Microsoft does not “support” JavaScript, and so does not allow you to turn it off.

### *Summing Up My Position*

The arguments against restricting Internet access are many, and at times they sound shrill. However, the fact remains that not everything on the Internet is appropriate for everybody, just as not every book or magazine published is appropriate for everybody. This being the case, some discrimination is called for in choosing what a public institution

makes available from the Internet. For example, even though libraries make many magazines available, they do not subscribe to *Hustler* because that would be

**“Do you prefer to be liable for ‘infringing’ on freedom of speech, or do you prefer to be liable for the effects of exposure to objectionable text and images?”**

an inappropriate addition to their collections. In this same vein, just because libraries provide access to the Internet, they do not need to provide access to the entire Internet.

I believe that much of the problem here stems from the differences between not subscribing to *Hustler* and not receiving Internet content that is pornographic, racist, or otherwise objectionable. In the former instance, you need do nothing to avoid a subscription; in the latter, action is necessary to keep pornographic content out of the library. The

need to take action in order to avoid questionable Internet material unfortunately confuses some people into mistaking positive proaction for repressive action. No one demands that libraries subscribe to *Hustler*, and so I feel that no one should

demand that libraries grant full and unrestricted access to the Internet to everyone.

Obviously, posted rules are not enough to limit access to pornography or other objectionable Internet content. Even those who do not want to access such content may have it forced on them. All this being the case, it behooves libraries to provide practical limits to Internet access. At present, filtering and/or blocking Internet content is the only means of even partially controlling access to offensive or objectionable material. Even though filtering sometimes results in legitimate sites being blocked—a problem that can be rectified manually—it is a practical action.

Those who might object on the basis of some specious “freedom of speech” issue should consider the Internet as an analog of real-world books and magazines. In that light, it is easy to see the absurdity of uncontrolled Internet access for children and other patrons. If the sort of content access that some advocate for the Internet were to be applied to conventional library content, *Hustler* magazine, neo-Nazi books and pamphlets, and worse objectionable material would have to be placed in juvenile and children’s as well as general library collections. This is what uncontrolled access to the Internet in a public venue can be. ☉

*Michael A. Banks, a resident of Oxford, Ohio, is the author of some 40 books, including The Internet Unplugged (see page 48). His other recent title, Web Psychos, Stalkers, and Pranksters: How to Protect Yourself in Cyberspace (The Coriolis Group, 1997), focuses on Internet crimes and privacy threats, and how to protect against them. The Web site for the books is <http://w3.one.net/~banks/psycho.htm>. His e-mail address is [75300.2721@compuserve.com](mailto:75300.2721@compuserve.com).*