MARJORIE HEINS, CHRISTINA CHO AND ARIEL FELDMAN

Internet Filters

A PUBLIC POLICY REPORT

SECOND EDITION, FULLY REVISED AND UPDATED
WITH A NEW INTRODUCTION

BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW

The Brennan Center for Justice, founded in 1995, unites thinkers and advocates in pursuit of a vision of inclusive and effective democracy. The Free Expression Policy Project founded in 2000, provides research and advocacy on free speech, copyright, and media democracy issues. FEPP joined the Brennan Center in 2004.

Michael Waldman
Executive Director

Deborah Goldberg
Director
Democracy Program

Marjorie Heins
Coordinator
Free Expression Policy Project

The Brennan Center is grateful to the Robert Sterling Clark Foundation, the Nathan Cummings Foundation, the Rockefeller Foundation, and the Andy Warhol Foundation for the Visual Arts for support of the Free Expression Policy Project.

Thanks to Kristin Glover, Judith Miller, Neema Trivedi, Samantha Frederickson, Jon Blitzer, and Rachel Nusbaum for research assistance.

Contents

Executive Summary

Every new technology brings with it both excitement and anxiety. No sooner was the Internet upon us in the 1990s than anxiety arose over the ease of accessing pornography and other controversial content. In response, entrepreneurs soon developed filtering products. By the end of the decade, a new industry had emerged to create and market Internet filters.

These filters were highly imprecise. The problem was intrinsic to filtering technology. The sheer size of the Internet meant that identifying potentially offensive content had to be done mechanically, by matching "key" words and phrases; hence, the blocking of Web sites for "Middle*sex* County," "*Beaver* College," and "*breast* cancer"—just three of the better-known among thousands of examples of overly broad filtering. Internet filters were crude and error-prone because they categorized expression without regard to its context, meaning, and value.

Some policymakers argued that these inaccuracies were an acceptable cost of keeping the Internet safe, especially for kids. Others—including many librarians, educators, and civil libertarians—argued that the cost was too high. To help inform this policy debate, the Free Expression Policy Project (FEPP) published a report in the fall of 2001 summarizing the results of more than 70 empirical studies on the performance of Internet filters. These studies ranged from anecdotal accounts of blocked sites to extensive research applying social-science methods.

Nearly every study revealed substantial overblocking. That is, even taking into account that filter manufacturers use broad and vague blocking categories—for example, "violence," "tasteless/gross," or "lifestyle"—their products arbitrarily and irrationally blocked many Web pages that had no relation to the disapproved content categories. For example:

- Net Nanny, SurfWatch, CYBERsitter, and Bess blocked House Majority Leader Richard "Dick" Armey's official Web site upon detecting the word "dick."
- SmartFilter blocked the Declaration of Independence, Shakespeare's complete plays, *Moby Dick*, and *Marijuana: Facts for Teens*, a brochure published by the National Institute on Drug Abuse.
- SurfWatch blocked the human rights site Algeria Watch and the University of Kansas's Archie R. Dykes Medical Library (upon detecting the word "dykes").
- CYBERsitter blocked a news item on the Amnesty International site after detecting the phrase "least 21." (The offending sentence described "at least 21" people killed or wounded in Indonesia.)
- X-Stop blocked Carnegie Mellon University's Banned Books page, the "Let's Have an Affair" catering company, and, through its "foul word" function, searches for *Bastard Out of Carolina* and "The Owl and the Pussy Cat."

Despite such consistently irrational results, the Internet filtering business continued to grow. Schools and offices installed filters on their computers, and public libraries came under pressure to do so. In December 2000, President Bill Clinton signed the "Children's Internet Protection Act," mandating filters in all schools and libraries that receive federal aid for Internet connections. The Supreme Court

upheld this law in 2003 despite extensive evidence that filtering products block tens of thousands of valuable, inoffensive Web pages.

The widespread use of filters presents a serious threat to our most fundamental free expression values.

In 2004, FEPP, now part of the Brennan Center for Justice at N.Y.U. School of Law, decided to update the *Internet Filters* report—a project that continued through early 2006. We found several large studies published during or after 2001, in addition to new, smaller-scale tests of filtering products. Studies by the U.S. Department of Justice, the Kaiser Family Foundation, and others found that despite improved technology and effectiveness in blocking some pornographic content, filters are still seriously flawed. They continue to deprive their users of many thousands of valuable Web pages, on subjects ranging from war and genocide to safer sex and public health. Among the hundreds of examples:

- WebSENSE blocked "Keep Nacogdoches Beautiful," a Texas cleanup project, under the category of "sex," and The Shoah Project, a Holocaust remembrance page, under the category of "racism/hate."
- Bess blocked all Google and AltaVista image searches as "pornography."
- Google's SafeSearch blocked congress.gov and shuttle.nasa.gov; a chemistry class at Middlebury College; Vietnam War materials at U.C.-Berkeley; and news articles from the *New York Times* and *Washington Post*.

The conclusion of the revised and updated *Internet Filters: A Public Policy Report* is that the widespread use of filters presents a serious threat to our most fundamental free expression values. There are much more effective ways to address concerns about offensive Internet content. Filters provide a false sense of security, while blocking large amounts of important information in an often irrational or biased way. Although some may say that the debate is over and that filters are now a fact of life, it is never too late to rethink bad policy choices.

Introduction to the Second Edition

The Origins of Internet Filtering

The Internet has transformed human communication. World Wide Web sites on every conceivable topic, e-newsletters and listservs, and billions of emails racing around the planet daily have given us a wealth of information, ideas, and opportunities for communication never before imagined. As the U.S. Supreme Court put it in 1997, "the content on the Internet is as diverse as human thought."[1]

Not all of this online content is accurate, pleasant, or inoffensive. Virtually since the arrival of the Internet, concerns have arisen about minors' access to online pornography, about the proliferation of Web sites advocating racial hatred, and about other online expression thought to be offensive or dangerous. Congress and the states responded in the late 1990s with censorship laws, but most of them were struck down by the courts. Partly as a result, parents, employers, school districts, and other government entities turned to privately manufactured Internet filters.

In the Communications Decency Act of 1996, for example, Congress attempted to block minors from Internet pornography by criminalizing virtually all "indecent" or "patently offensive" communications online. In response to a 1997 Supreme Court decision invalidating the law as a violation of the First Amendment,[2] the Clinton Administration began a campaign to encourage Internet filtering.

Early filtering was based on either "self-rating" by online publishers or "third-party rating" by filter manufacturers. Because of the Internet's explosive growth (by 2001, more than a billion Web sites, many of them changing daily)[3], and the consequent inability of filtering company employees to evaluate even a tiny fraction of it, third-party rating had to rely on mechanical blocking by key words or phrases such as "over 18," "breast," or "sex." The results were not difficult to predict: large quantities of valuable information and literature, particularly about health, sexuality, women's rights, gay and lesbian issues, and other important subjects, were blocked.

Even where filtering companies hired staff to review some Web sites, there were serious problems of subjectivity. The political attitudes of the filter manufacturers were reflected in their blocking decisions, particularly on such subjects as homosexuality, human rights, and criticism of filtering software. The alternative method, self-rating, did not suffer these disadvantages, but the great majority of online speakers refused to self-rate their sites. Online news organizations, for example, were not willing to reduce their content to simplistic letters or codes through self-rating.

Third-party filtering thus became the industry standard. From early filter companies such as SurfWatch and Cyber Patrol, the industry quickly expanded, marketing its products to school districts and corporate employers as well as families. Most of the products contained multiple categories of potentially

[1] *Reno v. ACLU*, 521 U.S. 844, 870 (1997), quoting *ACLU v. Reno*, 929 F. Supp. 824, 842 (E.D. Pa. 1996).

[2] *Id.*

[3] Two scholars estimated the size of the World Wide Web in January 2005 at more than 11.5 billion separate indexable pages. A. Gulli & A. Signorini, "The Indexable Web is More Than 11.5 Billion Pages" (May 2005). Source citations throughout this report do not include URLs if they can be found in the Bibliography.

offensive or "inappropriate" material. (Some had more than 50 categories.) Internet service providers such as America Online provided parental control options using the same technology.

Some manufacturers marketed products that were essentially "whitelists" — that is, they blocked most of the Internet, leaving just a few hundred or thousand pre-selected sites accessible. The more common configuration, though, was some form of blacklist, created through technology that trolled the Web for suspect words and phrases. Supplementing the blacklist might be a mechanism that screened Web searches as they happened; then blocked those that triggered words or phrases embedded in the company's software program.

The marketing claims of many filtering companies were exaggerated, if not flatly false. One company, for example, claimed that its "X-Stop" software identified and blocked only "illegal" obscenity and child pornography. This was literally impossible, since no one can be sure in advance what a court will rule "obscene." The legal definition of obscenity depends on subjective judgments about "prurience" and "patent offensiveness" that will be different for different communities.[4]

The "Children's Internet Protection Act" (CIPA)

The late 1990s saw political battles in many communities over computer access in public libraries. New groups such as Family Friendly Libraries attacked the American Library Association (ALA) for adhering to a no-censorship and no-filtering policy, even for minors. The ALA and other champions of intellectual freedom considered the overblocking of valuable sites by filtering software to be incompatible with the basic function of libraries, and advocated alternative approaches such as privacy screens and "acceptable use" policies. Meanwhile, anti-filtering groups such as the Censorware Project and Peacefire began to publish reports on the erroneous or questionable blocking of Internet sites by filtering products.

In December 2000, President Clinton signed the "Children's Internet Protection Act" (CIPA). CIPA requires all schools and libraries that receive federal financial assistance for Internet access through the e-rate or "universal service" program, or through direct federal funding, to install filters on all computers used by adults as well as minors.[5]

Technically, CIPA only requires libraries and schools to have a "technology protection measure" that prevents access to "visual depictions" that are "obscene" or "child pornography," or, for computers accessed by minors, depictions that are "obscene," "child pornography," or "harmful to minors."[6] But no "technological protection measure" (that is, no filter) can make these legal judgments, and even the narrowest categories offered by filter manufacturers, such as "adult" or "pornography," block both text and "visual depictions" that almost surely would not be found obscene, child pornography, or "harmful to minors" by a court of law.

[4] The Supreme Court defined obscenity for constitutional purposes in *Miller v. California*, 413 U.S. 15, 24 (1973). The three-part *Miller* test asks whether the work, taken as a whole, lacks "serious literary, artistic, political or scientific value"; whether, judged by local community standards, it appeals primarily to a "prurient" interest; and whether—again judged by community standards—it describes sexual organs or activities in a "patently offensive way."

[5] Public Law 106-554, §1(a)(4), 114 Stat. 2763A-335, amending 20 U.S. Code §6801 (the Elementary & Secondary Education Act); 20 U.S. Code §9134(b) (the Museum & Library Services Act); and 47 U.S. Code §254(h) (the e-rate provision of the Communications Act).

[6] "Harmful to minors" is a variation on the three-part obscenity test for adults (see note 4). CIPA defines it as: "any picture, image, graphic image file, or other visual depiction that
(i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
(ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
(iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors."
47 U.S. Code §254(h)(7)(G).

By delegating blocking decisions to private companies, CIPA thus accomplished far broader censorship than could be achieved through a direct government ban. As the evidence in the case that was brought to challenge CIPA showed, filters, even when set only to block "adult" or "sexually explicit" content, in fact block tens of thousands of nonpornographic sites.

CIPA does permit library and school administrators to disable the required filters "for bona fide research or other lawful purposes." The sections of the law that condition direct federal funding on the installation of filters allow disabling for minors and adults; the section governing the e-rate program only permits disabling for adults.[7]

CIPA put school and library administrators to a difficult choice: forgo federal aid in order to preserve full Internet access, or install filters in order to keep government grants and e-rate discounts. Not surprisingly, wealthy districts were better able to forgo aid than their lower-income neighbors. The impact of CIPA thus has fallen disproportionately on lower-income communities, where many citizens' only access to the Internet is in public schools and libraries. CIPA also hurts other demographic groups that are on the wrong side of the "digital divide" and that depend on libraries for Internet access, including people living in rural areas, racial minorities, and the elderly.

In 2001, the ALA, the American Civil Liberties Union, and several state and local library associations filed suit to challenge the library provisions of CIPA. No suit was brought to challenge the school provisions, and by 2005, the Department of Education estimated that 90% of K-12 schools were using some sort of filter in accordance with CIPA guidelines.[8]

A three-judge federal court was convened to decide the library suit. After extensive fact-finding on the operation and performance of filters, the judges struck down CIPA as applied to libraries. They ruled that the law forces librarians to violate their patrons' First Amendment right of access to information and ideas.

The decision included a detailed discussion of how filters operate. Initially, they trawl the Web in much the same way that search engines do, "harvesting" for possibly relevant sites by looking for key words and phrases. There follows a process of "winnowing," which also relies largely on mechanical techniques. Large portions of the Web are never reached by the harvesting and winnowing process.

The court found that most filtering companies also use some form of human review. But because 10,000-30,000 new Web pages enter their "work queues" each day, the companies' relatively small staffs (between eight and a few dozen people) can give at most a cursory review to a fraction of the sites that are harvested, and human error is inevitable.[9]

As a result of their keyword-based technology, the three-judge court found, filters wrongly block tens of thousands of valuable Web pages. Focusing on the three filters used most often in libraries — Cyber Patrol, Bess, and SmartFilter — the court gave dozens of examples of overblocking, among them: a Knights of Columbus site, misidentified by Cyber Patrol as "adult/sexually explicit"; a site on fly fishing, misidentified by Bess as "pornography"; a guide to allergies and a site opposing the death penalty, both blocked by Bess as "pornography"; a site for aspiring dentists, blocked by Cyber Patrol as "adult/sexually explicit"; and a site that sells religious wall hangings, blocked by WebSENSE as "sex."[10]

[7] 20 U.S. Code §6777(c); 20 U.S. Code §9134(f)(3); 47 U.S. Code §254(h)(6)(d).

[8] Corey Murray, "Overzealous Filters Hinder Research," *eSchool News Online* (Oct. 13, 2005).

[9] *American Library Association v. United States*, 201 F. Supp. 2d 401, 431-48 (E.D. Pa. 2002).

[10] *Id.*, 431-48.

The judges noted also that filters frequently block all pages on a site, no matter how innocent, based on a "root URL." The root URLs for large sites like Yahoo or Geocities contain not only educational pages created by nonprofit organizations, but thousands of personal Web pages. Likewise, the court found, one item of disapproved content — for example, a sexuality column on Salon.com — often results in blocking of the entire site.[11]

The trial court struck down CIPA's library provisions as applied to both adults and minors. It found that there are less burdensome ways for libraries to address concerns about illegal obscenity on the Internet, and about minors' access to material that most adults consider inappropriate for them — including "acceptable use" policies, Internet use logs, and supervision by library staff.[12]

The government appealed the decision of the three-judge court, and in June 2003, the Supreme Court reversed, upholding the constitutionality of CIPA. Chief Justice William Rehnquist's opinion (for a "plurality" of four of the nine justices) asserted that library patrons have no right to unfiltered Internet access — that is, filtering is no different, in principle, from librarians' decisions not to select certain books for library shelves. Moreover, Rehnquist said, because the government is providing financial aid for Internet access, it can limit the scope of the information that is accessed. He added that if erroneous blocking of "completely innocuous" sites creates a First Amendment problem, "any such concerns are dispelled" by CIPA's provision giving libraries the discretion to disable the filter upon request from an adult.[13]

Justices Anthony Kennedy and Stephen Breyer wrote separate opinions concurring in the judgment upholding CIPA. Both relied on the "disabling" provisions of the law as a way for libraries to avoid restricting adults' access to the Internet. Kennedy emphasized that if librarians fail to unblock on request, or adults are otherwise burdened in their Internet searches, then a lawsuit challenging CIPA "as applied" to that situation might be appropriate.[14]

Three justices—John Paul Stevens, David Souter, and Ruth Bader Ginsberg—dissented from the Supreme Court decision upholding CIPA. Their dissents drew attention to the district court's detailed description of how filters work, and to the delays and other burdens that make discretionary disabling a poor substitute for unfettered Internet access. Souter objected to Rehnquist's analogy between Internet filtering and library book selection, arguing that filtering is actually more akin to "buying an encyclopedia and then cutting out pages." Stevens, in a separate dissent, noted that censorship is not necessarily constitutional just because it is a condition of government funding—especially when funded programs are designed to facilitate free expression, as in universities and libraries, or on the Internet.[15]

Living with CIPA

After the Supreme Court upheld CIPA, public libraries confronted a stark choice — forgo federal aid, including e-rate discounts, or invest resources in a filtering system that, even at its narrowest settings, will censor large quantities of valuable material for reasons usually known only to the manufacturer. The ALA and other groups began developing information about different filtering products, and suggestions for choosing products and settings that block as little of the Internet as possible, consistent with CIPA.

These materials remind librarians that

[11] *Id.*

[12] *Id.*, 480-84.

[13] *U.S. v. American Library Association*, 123 S. Ct. 2297, 2304-09 (2003) (plurality opinion).

[14] *Id.*, 2309-12 (concurring opinions of Justices Kennedy and Breyer).

[15] *Id.*, 2317, 2321-22 (dissenting opinions of Justices Stevens and Souter).

whatever filter system they choose should allow configuration of the default page to educate the user on how the filter works and how to request disabling. Libraries should adopt systems that can be easily disabled, in accordance with the Supreme Court's statement that CIPA doesn't violate the First Amendment in large part because it authorizes librarians to disable filters on the request of any adult.[16]

In order to avoid commercial products that maintain secret source codes and blacklists, the Kansas library system developed its own filter, KanGuard. Billed as "a library-friendly alternative," KanGuard was created by customizing the open-source filter SquidGuard, and aims to block only pornography. But although KanGuard's and SquidGuard's open lists may make it easier for administrators to unblock nonpornographic sites that are erroneously targeted, they cannot avoid the errors of the commercial products, since they rely on essentially the same technology.[17]

How have libraries responded to CIPA? According to reports collected by the ALA, some systems have decided to forgo federal aid or e-rate discounts rather than install filters. One of them, in San Francisco, is subject to a city ordinance that "explicitly bans the filtering of Internet content on adult and teen public access computers." A librarian at the San Francisco Public Library explained that although the ban could cost the library up to $225,000 in lost e-rate funds, the "community doesn't want filtering."[18]

Likewise, several libraries in New Hampshire decided to forgo federal aid. They were encouraged by the New Hampshire Library Association, which posted a statement on its Web site noting that filters block research on breast cancer, sexually transmitted diseases, "and even Super Bowl XXX."[19]

These libraries were the exception, though. A preliminary study by the ALA and the Center for Democracy and Technology in 2004, based on a sample of about 50 libraries, indicated that a large majority now use filters, "and most of the filtering is motivated by CIPA requirements." Only 11% of the libraries that filter confine their filters to the children's section. 64% will disable the filter upon request, but fewer than 20% will disable the filter for minors as well as adults.[20] This picture contrasts sharply with the situation before the Supreme Court's decision upholding CIPA, when researchers reported that 73% of libraries overall, and 58% of public libraries, did not use filters. 43% of the public libraries were receiving e-rate discounts; only 18.9% said they would not continue to apply for the e-rate should CIPA be upheld.[21]

In 2005, the Rhode Island affiliate of the American Civil Liberties Union reported that before the Supreme Court upheld CIPA, fewer than ¼ of the libraries in the state that responded to its survey had installed Internet filters, and many had official policies

[16] *E.g.*, Lori Bowen Ayre, *Filtering and Filter Software* (ALA Library Technology Reports, 2004); Open Net Initiative, "Introduction to Internet Filtering" (2004); Derek Hansen, "CIPA: Which Filtering Software to Use?" (Aug. 31, 2003).

[17] The coordinator of the system says that KanGuard's lists are compiled "with an open-source 'robot' program that scours the Web, searching for language and images that are clearly obscene or harmful to minors." Walter Minkel, "A Filter That Lets Good Information In," *TechKnowledge* (Mar. 1, 2004). But no "robot" looking for language or images can make these legal determinations, and SquidGuard admits that its blacklists "are entirely the product of a dumb robot. We strongly recommend that you review the lists before using them." "The SquidGuard Blacklist," www.squidguard.org/blacklist (visited 4/3/05). As of 2005, the "porn" section of SquidGuard had more than 100,000 entries.

[18] Joseph Anderson, "CIPA and San Francisco: Why We Don't Filter," *WebJunction* (Aug. 31, 2003).

[19] Associated Press, "Libraries Oppose Internet Filters, Turn Down Federal Funds" (June 13, 2004).

[20] Center for Democracy & Technology & ALA, "Children's Internet Protection Act Survey: Executive Summary" (2004) (on file at the Free Expression Policy Project).

[21] Paul Jaeger, John Carlo Bertot, & Charles McClure, "The Effects of the Children's Internet Protection Act (CIPA) in Public Libraries and its Implications for Research: A Statistical, Policy, and Legal Analysis," 55(13) *Journal of the American Society for Information Science and Technology* 1131, 1133 (2004).

prohibiting them. By July 1, 2004, however—the government's deadline for implementing CIPA — all of them were using the WebSENSE filter, as recommended by the statewide consortium responsible for Internet access in libraries.[22]

Although each library system in Rhode Island is allowed to choose its own filter settings, the survey showed that most of them followed the consortium's recommendations and configured WebSENSE to block the "sex," "adult content," and "nudity" categories. Four libraries blocked additional categories such as "gambling," "games," "personals and dating," and "chat." And even though the Supreme Court conditioned its approval of CIPA on the ability of libraries to disable filters on request, the survey found that many of the state's library directors were confused about disabling their filter and had received no training on how to do so. More than ⅓ of them said they did not notify patrons that the filters could be disabled or even that they were in use.[23]

The Rhode Island ACLU concluded with four recommendations on how to minimize CIPA's impact on access to information:

- Filters should be set at the minimum blocking level necessary to comply with the law;
- Libraries should notify patrons that they have a right to request that the filter be disabled;
- Libraries should train their staff on how to disable the filter and on patrons' right to request disabling; and
- All adult patrons should be given the opportunity to use an unfiltered Internet connection.[24]

[22] Amy Myrick, *Reader's Block: Internet Censorship in Rhode Island Public Libraries* (Rhode Island ACLU, 2005).

[23] Myrick, 16. Moreover, on two occasions when a researcher asked a librarian at the Providence Public library to unblock a wrongly blocked site, the librarian refused and subjected the researcher to judgmental comments and questioning about the site's subject matter. *Id.*, 15.

[24] *Id.*, 17.

Public schools also have to deal with the complexities and choices occasioned by CIPA. In 2001, the Consortium for School Networking (CoSN) published a primer, *Safeguarding the Wired Schoolhouse*, directed at policymakers in K-12 schools. The primer seemed to accept filtering as a political necessity in many school districts; after Congress passed CIPA, of course, it became a legal necessity as well. CoSN's later materials outline school districts' options, but note that its resources "should not be read as an endorsement of [CIPA], of content controls in general, or of a particular technological approach."[25]

A further indication of the educational environment came from a reporter who observed:

> Many school technology coordinators argue that the inexact science of Internet filtering and blocking is a reasonable trade-off for greater peace of mind. Given the political reality in many school districts, they say, the choice often comes down to censorware or no Internet access at all.

He quotes an administrator as saying: "It would be politically disastrous for us not to filter. All the good network infrastructure we've installed would come down with the first instance of an elementary school student accessing some of the absolutely raunchy sites out there."[26]

Yet studies indicate that filters in schools also frustrate legitimate research and exacerbate the digital divide.[27] The more privileged

[25] "School District Options for Providing Access to Appropriate Internet Content" (power point), www.safewiredschools.org/pubs_and_tools/sws_powerpoint.ppt (visited 2/21/06); *Safeguarding the Wired Schoolhouse* (CoSN, June 2001).

[26] Lars Kongshem, "Censorware—How Well Does Internet Filtering Software Protect Students?" *Electronic School Online* (Jan. 1998) (quoting Joe Hill, supervisor at Rockingham County, Virginia Public Schools).

[27] See the reports of the Electronic Frontier Foundation/Online Policy Group and the Kaiser Family Foundation; and the PhD Dissertation of Lynn Sutton, pages 66, 62, 70.

students, who have unfiltered Internet access at home, are able to complete their research projects. The students from less prosperous homes are further disadvantaged in their educational opportunities.

Filtering Studies During and After 2001

By 2001, some filter manufacturers said that they had corrected the problem of overblocking, and that instead of keywords, they were now using "artificial intelligence." But no matter how impressive-sounding the terminology, the fact remains that all filtering depends on mechanical searches to identify potentially inappropriate sites. Although some of the sillier technologies—such as blocking one word in a sentence and thereby changing the entire meaning[28]—are less often seen today, studies have continued to document the erroneous blocking of thousands of valuable Web sites, much of it clearly due to mechanical identification of key words and phrases.[29]

The first edition of *Internet Filters: A Public Policy Report* was intended to advance informed debate on the filtering issue by summarizing all of the studies and tests to date, in one place and in readily accessible form. This second edition brings the report up-to-date, with summaries of new studies and additional background on the filtering dilemma.

Part I is a revision of our 2001 report, and is organized by filtering product. Necessarily, there is some overlap, since many studies sampled more than one product. We have updated the entries to reflect changes in blocking categories, or the fact that some of the filters mentioned are no longer on the market. In the interest of space, we have omitted an appendix from the 2001 report listing blocked sites according to subject: artistic and literary sites; sexuality education; gay and lesbian information; political topics; and sites relating to censorship itself. This appendix is available online at www.fepproject.org/policyreports/appendixa.html.

Part II describes the tests and studies published during or after 2001. Several of these are larger and more ambitious than the earlier studies, and combine empirical results with policy and legal analysis. Our summaries of these more complex reports are necessarily longer than the summaries in the 2001 research scan. We have focused on the empirical results and sometimes, in the interest of readability, have rounded off statistics to the nearest whole number. We urge readers to consult the studies themselves for further detail.

Some of the reports described in Part II attempt to estimate the overall statistical accuracy of different filtering products. Filtering companies sometimes rely on these reports to boast that their percentage of error is relatively small. But reducing the problems of over- and underblocking to numerical percentages is problematic.

For one thing, percentages and statistics can be easily manipulated. Since it is very difficult to create a truly random sample of Web sites for testing, the rates of over- and underblocking will vary depending on what sites are chosen. If, for example, the test sample has a large proportion of nonpornographic educational sites on a controversial topic such as birth control, the error rate will likely be much higher than if the sample has a large number of sites devoted to children's toys. Overblocking rates will also vary depending on the denominator of the fraction—that is, whether the number of wrongly blocked sites is compared to the overall total of blocked sites or to the overall total of sites tested.[30]

[28] The most notorious example was CYBERsitter's blocking the word "homosexual" in the phrase: "The Catholic Church opposes homosexual marriage" (see page 22).

[29] In addition to the primary research reports described in Part II, see Commission on Child Online Protection (COPA), *Report to Congress*, (Oct. 20, 2000); National Research Council, *Youth, Pornography, and the Internet* (2002).

[30] See the discussion of Resnick *et al.*'s article on test methodology, page 45.

Moreover, even when researchers report a relatively low error rate, this does not mean that the filter is a good tool for libraries, schools, or even homes. With billions of Internet pages, many changing daily, even a 1% error rate can result in millions of wrongly blocked sites.

Finally, there are no consistent or agreed-upon criteria for measuring over- and underblocking. As we have seen, no filter can make the legal judgments required by CIPA. But even if errors are measured based on the content categories created by filter manufacturers, it is not always easy for researchers to decide whether particular blocked pages fit within those categories. Percentage summaries of correctly or incorrectly blocked sites are often based on mushy and variable underlying judgments about what qualifies as, for example, "alternative lifestyle," "drug culture," or "intolerance."

Because of these difficulties in coming up with reliable statistics, and the ease with which error rates can be manipulated, we believe that the most useful research on Internet filters is cumulative and descriptive—that is, research that reveals the multitude of sites that are blocked and the types of information and ideas that filters censor from view.

Since the first edition of *Internet Filters*, the market for these products has expanded enormously. In our original research, we found studies that tested one or more of 19 different filters. In 2005, we found 133 filtering products. Some of them come in multiple formats for home, school, or business markets. But there are probably fewer than 133 separate products, because the basic software for popular filters like Bess and Cyber Patrol is licensed to Internet service providers and other companies that want to offer filtering under their own brand name.

Many companies now offer all-purpose "Web protection" tools that combine censorship-based filters with other functions such as screening out spam and viruses. Security screening tools have become necessary on the Internet, but they are quite different from filters that block based not on capacity to harm a computer or drown a user's mailbox with spam, but on a particular manufacturer's concept of offensiveness, appropriateness, or child protection.

The Continuing Challenge

Internet filtering continues to be a major policy issue, and a challenge for our system of free expression. Some might say that the debate is over and that despite their many flaws, filters are now a fact of life in American homes, schools, offices, and libraries. But censorship on such a large scale, controlled by private companies that maintain secret blacklists and screening technologies, should always be a subject of debate and concern.

We hope that the revised and updated *Internet Filters* will be a useful resource for policymakers, parents, teachers, librarians, and all others concerned with the Internet, intellectual freedom, or the education of youth. Internet filtering is popular, despite its unreliability, because many parents, political leaders, and educators feel that the alternative—unfettered Internet access—is even worse. But to make these policy choices, it is necessary to have accurate information about what filters do. Ultimately, as the National Research Council observed in a 2002 report, less censorial approaches such as media literacy and sexuality education are the only effective ways to address concerns about young people's access to controversial or disturbing ideas.[31]

[31] National Research Council, *Youth, Pornography, and the Internet*, Exec. Summary; ch. 10.

I. The 2001 Research Scan Updated: Over- and Underblocking by Internet Filters

This section is organized by filtering product, and describes each test or study that we found up through the fall of 2001.

America Online Parental Controls

AOL offers three levels of Parental Controls: "Kids Only," for children 12 and under; "Young Teen," for ages 13-15; and "Mature Teen," for ages 16-17, which allows access to "all content on AOL and the Internet, except certain sites deemed for an adult (18+) audience."[32] AOL encourages parents to create unique screen names for their children and to assign each name to one of the four age categories. At one time, AOL employed Cyber Patrol's block list; at another point it stated it was using SurfWatch. In May 2001, AOL announced that Parental Controls had integrated the RuleSpace Company's "Contexion Services," which identifies "objectionable" sites "by analyzing both the words on a page and the context in which they are used."[33]

Gay and Lesbian Alliance Against Defamation (GLAAD), *Access Denied, Version 2.0: The Continuing Threat Against Internet Access and Privacy and Its Impact on the Lesbian, Gay, Bisexual and Transgender Community* (1999)

This 1999 report was a follow-up to GLAAD's 1997 publication, *Access Denied: The Impact of Internet Filtering Software on the Lesbian and Gay Community*, which described the defects of various filtering products without identifying particular blocked sites. *Access Denied, Version 2.0* addressed AOL Parental Controls only in its introduction, where it reported that the "Kids Only" setting blocked the Web site of Children of Lesbians and Gays Everywhere (COLAGE), as well as a number of "family, youth and national organization Web sites with lesbian and gay content," none of which were named in the report.

Brian Livingston, "AOL's 'Youth Filters' Protect Kids From Democrats," *CNet News* (Apr. 24, 2000)

Livingston investigated AOL's filtering for signs of political bias. He found that the "Kids Only" setting blocked the Web sites of the Democratic National Committee, the Green Party, and Ross Perot's Reform Party, but not those of the Republican National Committee and the conservative Constitution and Libertarian parties. AOL's "Young Teen" setting blocked the home pages of the Coalition to Stop Gun Violence, Safer Guns Now, and the Million Mom March, but neither the National Rifle Association site nor the commercial sites for Colt & Browning firearms.

Bennett Haselton, "AOL Parental Controls Error Rate for the First 1,000 .com Domains" (Peacefire, Oct. 23, 2000)

Peacefire Webmaster Bennett Haselton tested AOL Parental Controls on 1,000 dot-com domains he had compiled for a similar test of SurfWatch two months earlier (see page 36). He attempted to access each site on AOL

[32] AOL, "Parental Controls," site.aol.com/info/parentcontrol.html (visited 3/6/06).

[33] AOL press release, "AOL Deploys RuleSpace Technology Within Parental Controls" (May 2, 2001), www.rulespace.com/news/pr107.php (visited 2/23/06).

5.0 adjusted to its "Mature Teen" setting. Five of the 1,000 working domains were blocked, including a-aji.com, a site that sold vinegar and seasonings. Haselton decided the four others were pornographic and thus accurately blocked. This produced an "error rate" of 20%, the lowest, by Peacefire's calculation, of the five filters tested. AOL also "blocked far fewer pornographic sites than any of the other programs," however. Haselton stated that five blocked domains was an insufficient sample to gauge the efficacy of AOL Parental Controls accurately, and that the true error rate could fall anywhere between 5-75%.

"Digital Chaperones for Kids," *Consumer Reports* (Mar. 2001)

Consumer Reports assessed AOL's "Young Teen" and "Mature Teen" settings along with various other filtering technologies. For each filter, the researchers attempted to access 86 Web sites that they deemed objectionable because of "sexually explicit content or violently graphic images," or promotion of "drugs, tobacco, crime, or bigotry." They also tested the filters against 53 sites they deemed legitimate because they "featured serious content on controversial subjects." The "Mature Teen" setting left 30% of the "objectionable" sites unblocked; the "Young Teen" filter failed to block 14% – the lowest underblocking rate of all products reviewed. But "Young Teen" also blocked 63% of the "legitimate" sites, including Peacefire.org; Lesbian.org, an online guide to lesbian politics, history, arts, and culture; the Citizens' Committee for the Right to Keep and Bear Arms; the Southern Poverty Law Center; and *SEX, Etc.*, a sex education site hosted by Rutgers University.

Miscellaneous Reports

- In "BabelFish Blocked by Censorware" (Feb. 27, 2001), Peacefire reported that AOL's "Mature Teen" setting barred access to BabelFish, AltaVista's foreign-language translation service.

Bess

Bess, originally manufactured by N2H2, was acquired by Secure Computing in October 2003. By late 2005, Bess had been merged into SmartFilter, another Secure Computing product, and was being marketed to schools under the name SmartFilter, Bess Edition.[34]

Bess combines technology with some human review. Although N2H2 initially claimed that all sites were reviewed by its employees before being added to the block list, the current promotional literature simply states that the filter's "unique combination of technology and human review … reduces frustrations associated with 'keyword blocking' methods, including denied access to sites regarding breast cancer, sex education, religion, and health."[35]

In 2001, Bess had 29 blocking categories; by 2006, the number was 38, ranging from "adults only" and "alcohol" to "gambling," "jokes," "lingerie," and "tasteless/gross." Its four "exception" categories in 2001 were expanded to six: "history," "medical," "moderated," "text/spoken only," "education," and "for kids." Each exception category allows access to sites that have educational value but might otherwise be filtered – for example, children's games that would be blocked under "games" or "jokes"; classic literature, history, art, or sex education that would be blocked under "sex," "nudity," or "violence."

Karen Schneider, *A Practical Guide to Internet Filters* (1997)

From April to September 1997, Karen Schneider supervised a nationwide team of librarians in testing 13 filters, including Bess.

[34] "Secure Computing Acquires N2H2," www.securecomputing.com/index.cfm?skey=1453 (visited 3/3/06). Secure Computing also embeds filtering for "inappropriate" content in other pr.oducts such as CyberGuard and Webwasher. "Secure Computing Products at a Glance," www.bess.com/index.cfm?skey=496; www.securecomputing.com/index.cfm?skey=496 (visited 3/3/06).

[35] "SmartFilter, Bess Edition, Filtering Categories," www.bess.com/index.cfm?skey=1379 (visited 3/3/06).

The results of this Internet Filter Assessment Project, or TIFAP, were published later that year in Schneider's *Practical Guide to Internet Filters*.

The researchers began by seeking answers to 100 common research queries, on both unfiltered computers and ones equipped with Bess (and the various other filters) configured for maximum blocking, including keyword blocking. Each query fell into one of 11 categories: "sex and pornography,'" "anatomy," "drugs, alcohol, and tobacco," "gay issues," "crimes (including pedophilia and child pornography)," "obscene or 'racy' language," "culture and religion," "women's issues," "gambling," "hate groups and intolerance," and "politics." The queries were devised to gauge filters' handling of controversial issues – for instance, "I'd like some information on safe sex"; "I want information on the legalization of marijuana"; "Is the Aryan Nation the same thing as Nazis?" and "Who are the founders of the Electronic Frontier Foundation and what does it stand for?" In some cases, the queries contained potentially provocative terms "intended to trip up keyword-blocking mechanisms," such as "How do beavers make their dams?"; "Can you find me some pictures from *Babes in Toyland*?"; and "I'm trying to find out about the Paul Newman movie *The Hustler*."

Schneider used Web sites, blocked and unblocked, that arose from these searches to construct a test sample of 240 URLs. Her researchers tested these URLs against a version of Bess configured for "maximum filtering," but with keyword filtering disabled. TIFAP found that "several" (Schneider did not say how many) nonpornographic sites were blocked, including a page discussing X-rated videos but not containing any pornographic imagery, and an informational page on trichomaniasis, a vaginal disease. Upon notification and review, Bess later unblocked the trichomaniasis site. *A Practical Guide* included neither the names nor the Web addresses of the blocked sites.

Censorware Project, *Passing Porn, Banning the Bible: N2H2's Bess in Public Schools* (2000)

From July 23-26, 2000, the Censorware Project tested "thousands" of URLs against 10 Bess proxy servers, seven of which were in use in public schools across the United States. Among the blocked sites were a page from *Mother Jones* magazine; the Institute of Australasian Psychiatry; the nonprofit effort Stop Prisoner Rape; and a portion of the Columbia University Health Education Program site, on which users are invited to submit "questions about relationships; sexuality: sexual health; emotional health; fitness; nutrition; alcohol, nicotine, and other drugs; and general health." Bess also blocked the United Kingdom-based Feminists Against Censorship, the personal site of a librarian opposing Internet filter use in libraries, and *Time* magazine's "Netly News," which had reported, positively and negatively, on filtering software.

The report noted that, contrary to the implication in Bess's published filtering criteria, Bess does not review home pages hosted by such free site providers as Angelfire, Geocities, and Tripod (owing, it seems, to their sheer number). Instead, users must configure the software to block none or all of these sites; some schools opt for the latter, thus prohibiting access to such sites as *The Jefferson Bible*, a compendium of Biblical passages selected by Thomas Jefferson, and the Eustis Panthers, a high school baseball team. Though each proxy was configured to filter out pornography to the highest degree, Censorware reported that it was able to access hundreds of pornographic Web sites, of which 46 are listed in *Passing Porn*.

Peacefire, "'BESS, the Internet Retriever' Examined" (2000; since updated)

This report lists 15 sites that Peacefire deemed inappropriately blocked by Bess

during the first half of 2000. They included Peacefire.org itself, which was blocked for "Profanity" when the word "piss" appeared on the site (in a quotation from a letter written by Brian Milburn, president of CYBERsitter's manufacturer, Solid Oak Software, to journalist Brock Meeks). Also blocked were: two portions of the Web site of Princeton University's Office of Population Research; the Safer Sex page; five gay-interest sites, including the home page of the Illinois Federation for Human Rights; two online magazines devoted to gay topics; two Web sites providing resources on eating disorders; and three sites discussing breast cancer.[36]

Jamie McCarthy, "Mandated Mediocrity: Blocking Software Gets a Failing Grade" (Peacefire/ Electronic Privacy Information Center, Oct. 2000)

"Mandated Mediocrity" describes another 23 Web sites inappropriately blocked by Bess. The URLs were tested against an N2H2 proxy as well as a trial copy of the N2H2 Internet Filtering Manager set to "typical school filtering." Among the blocked sites were the Traditional Values Coalition; "Hillary for President"; "The Smoking Gun," an online

Bess blocked the Traditional Values Coalition and "Hillary for President."

selection of primary documents relating to current events; a selection of photographs of Utah's national parks; "What Is Memorial Day?", an essay lamenting the "capitalistic American" conception of the holiday as nothing more than an occasion for a three-day weekend; the home page of "American Government and Politics," a course at St. John's University; and the Circumcision Information and Research Pages, a site that contained no nudity and was designated a "Select Parenting Site" by ParenthoodWeb.com.

Bennett Haselton, "BESS Error Rate for 1,000 .com Domains" (Peacefire, Oct. 23, 2000)

Bennett Haselton performed the same test of 1,000 active dot-com domains for Bess as he did for AOL (see page 9). N2H2 officials had evidently reviewed his earlier report on SurfWatch, and prepared for a similar test by unblocking any of the 1,000 sites inappropriately filtered by Bess,[37] so Peacefire selected a second 1,000 dot-com domains for testing against a Bess proxy server in use at a school where a student had offered to help measure Bess's performance.

The filter was configured to block sites in the categories of "adults only," "alcohol," "chat," "drugs," "free pages," "gambling," "hate/discrimination," "illegal," "lingerie," "nudity," "personals," "personal information," "porn site," "profanity," "school cheating info," "sex," "suicide/murder," "tasteless/gross," "tobacco," "violence," and "weapons." The keyword-blocking features were also enabled. The BESS proxy blocked 176 of the 1,000 domains; among these, 150 were "under construction." Of the remaining 26 sites, Peacefire deemed seven wrongly blocked: a-celebrity.com, a-csecurite.com, a-desk.com, a-eda.com, a-gordon.com, a-h-e.com, and a-intec.com.

The report said the resulting "error rate" of 27% was unreliable given how small a sample was examined; the true error rate "could be as low as 15%." Haselton also noted that the dot-com domains tested here were "more likely to contain commercial pornography than, say, .org domains. ... We should expect

[36] These last three pages were not filtered because of an automatic ban on the keyword "breast," but either were reviewed and deemed unacceptable by a Bess employee, or had other words or phrases that triggered the filter. The report noted: "In our tests, we created empty pages that contained the words *breast* and *breast cancer* in the titles, to test whether Bess was using a word filter. The pages we created were accessible, but the previous three sites about breast cancer were still blocked."

[37] Bennett Haselton, "Study of Average Error Rates for Censorware Programs" (Peacefire, Oct. 23, 2000).

the error rate to be even *higher* for .org sites." He added that the results called into question N2H2 CEO Peter Nickerson's claim, in 1998 testimony before a congressional committee, that "all sites that are blocked are reviewed by N2H2 staff before being added to the block lists."[38]

Bennett Haselton & Jamie McCarthy, "Blind Ballots: Web Sites of U.S. Political Candidates Censored by Censorware" (Peacefire, Nov. 7, 2000)

"Blind Ballots" was published on Election Day, 2000. The authors obtained a random sample of political candidates' Web sites from NetElection.org, and set out to see which sites Bess's (and Cyber Patrol's) "typical school filtering" would allow users to access. (Around the start of the 2000 school year, Bess and Cyber Patrol asserted that together they were providing filtered Internet access to more than 30,000 schools nationwide.[39])

Bess's wholesale blocking of free Web hosting services caused the sites of one Democratic candidate, five Republicans, six Libertarians (as well as the entire Missouri Libertarian Party site), and 13 other third-party candidates to be blocked. The authors commented that, as "many of our political candidates run their campaigns on a shoestring, and use free-hosting services to save money," Bess's barring of such hosts leads it to an inadvertent bias toward wealthy or established politicians' sites. Congressman Edward Markey (a Democrat from Massachusetts), also had his site blocked – unlike the others, it was not hosted by Geocities or Tripod, but was blocked because Bess categorized its content as "hate, illegal, pornography, and/or violence." "While blocking software companies often justify their errors by pointing out that they are quickly corrected," the report concluded, "this does not help any of the candidates listed above. ... corrections made after Election Day do not help them at all."

Bennett Haselton, "Amnesty Intercepted: Global Human Rights Groups Blocked by Web Censoring Software" (Peacefire, Dec. 12, 2000)

In response to complaints from students barred from the Amnesty International Web page, among others, at their school computer stations, Peacefire examined various filters' treatment of human rights sites. It found that Bess's "typical school filtering" blocked the home pages of the International Coptic Congress, which tracked human rights violations against Coptic Christians living in Egypt; and Friends of Sean Sellers, which contained links to the works of the Multiple Personality Disorder-afflicted writer who was executed in 1999 for murders he had committed as a 16-year-old. (The site opposed capital punishment.)

"Typical school filtering" also denied access to the official sites of recording artists Suzanne Vega and the Art Dogs; both contained statements that portions of their proceeds would be donated to Amnesty International. Bess's "minimal filtering" configuration blocked the Web sites of Human Rights & Tamil People, which tracks government and police violence against Hindu Tamils in Sri Lanka; and Casa Alianza, which documents the condition of homeless children in the cities of Central America.

Miscellaneous Reports

- In its "Winners of the Foil the Filter Contest" (Sept. 28, 2000), the Digital Freedom Network reported that Bess blocked House Majority Leader Richard "Dick" Armey's official Web site upon detecting the word

[38] Peter Nickerson Testimony, House Subcom. on Telecommunications, Trade, and Consumer Protection (Sept. 11, 1998), www.peacefire.org/censorware/BESS/peter-nickerson.filtering-bill-testimony.9-11-1998.txt (visited 3/6/06).

[39] N2H2 press release, "N2H2 Launches Online Curriculum Partners Program, Offers Leading Education Publishers Access to Massive User Base" (Sept. 6, 2000); Surf Control press release, "Cyber Patrol Tells COPA Commission that Market for Internet Filtering Software to Protect Kids is Booming" (July 20, 2000).

"dick." Armey, himself a filtering advocate, won "The Poetic Justice Award – for those bitten by their own snake."

- Peacefire reported, in "BabelFish Blocked by Censorware" (Feb. 27, 2001), that Bess blocked the URL-translation site BabelFish.
- In "Teen Health Sites Praised in Article, Blocked by Censorware" (Mar. 23, 2001), Peacefire's Bennett Haselton noted that Bess blocked portions of TeenGrowth, a teen-oriented health education site that was recognized by the *New York Times* in the recent article, "Teenagers Find Health Answers with a Click."[40]

ClickSafe

Rather than relying on a list of objectionable URLs, ClickSafe software reviewed each requested page in real time. In an outline for testimony submitted to the commission created by the 1998 Child Online Protection Act (the "COPA Commission"), company co-founder Richard Schwartz claimed that ClickSafe "uses state-of-the-art, content-based filtering software that combines cutting edge graphic, word and phrase-recognition technology to achieve extraordinarily high rates of accuracy in filtering pornographic content," and "can precisely distinguish between appropriate and inappropriate sites."[41] This was vigorously disputed by Peacefire (see below). By 2005, a Web site for the ClickSafe filter could no longer be found, although a European company using the same name had launched a site focused on Internet safety for minors.[42]

Peacefire, "Sites Blocked by ClickSafe" (July 2000)

Upon learning that ClickSafe blocked the home page of cyberlaw scholar Lawrence Lessig, who was to testify before the COPA Commission, Peacefire attempted to access various pages on the COPA Commission site, as well as the Web sites of organizations and companies with which the commissioners were affiliated, through a computer equipped with ClickSafe. On the Commission's site, ClickSafe blocked the Frequently Asked Questions page; the biographies of Commission members Stephen Balkam, Donna Rice Hughes, and John Bastian; a list of "technologies and methods" within the scope of the Commission's inquiry; the Commission's Scope and Timeline Proposal; and two versions of the COPA law.

As for groups with representatives on the Commission, ClickSafe blocked several organizations' and companies' sites, at least partially: Network Solutions; the Internet Content Rating Association; Security Software's information page on its signature filtering product, Cyber Sentinel; FamilyConnect, a brand of blocking software; the National Law Center for Children and Families; the Christian site Crosswalk.com; and the Center for Democracy and Technology (CDT). In addition to the CDT, ClickSafe blocked the home pages of the ACLU, the Electronic Frontier Foundation, and the American Family Association, as well as part of the official site for Donna Rice Hughes's book, *Kids Online: Protecting Your Children in Cyberspace*.

Cyber Patrol

In 2001, Cyber Patrol operated with 12 default blocking categories, including "partial nudity," "intolerance," "drugs/drug culture," and "sex education."[43] The manufacturer's Web site in 2001 implied that "a team of professional researchers" reviewed all sites to decide whether they should be blocked; by 2006, the company described its filter as a mix

[40] Bonnie Rothman Morris, "Teenagers Find Health Answers with a Click," *New York Times* (Mar. 20, 2001), F8.

[41] Outline for Testimony Presented by Richard Schwartz, Co-Founder, ClickSafe.com, www.copacommission.org/meetings/hearing2/schwartz.test.pdf (visited 3/13/05).

[42] "New Clicksafe" (site in Dutch and French), www.clicksafe.be/taalkeuze.html (visited 3/13/05); "Background Clicksafe," www.saferinternet.org/ww/en/pub/insafe/focus/belgium/be_node.htm (visited 3/13/05).

[43] By 2005, Cyber Patrol had 13 categories, several of them different from the original 12. CyberList, www.cyberpatrol.com/Default.aspx?id=123&mnuid=2.5 (visited 3/14/06).

of human researchers and automated tools.[44] Like most filter manufacturers, Cyber Patrol does not make its list of prohibited sites public, but its "test-a-site" search engine (formerly called "CyberNOT") allows users to enter URLs and learn immediately whether those pages are on the list. In 2001, the company stated that it blocked all Internet sites "that contain information or software programs designed to hack into filtering software" in *all* of its blocking categories; this statement is no longer on the Cyber Patrol site.

Brock Meeks & Declan McCullagh, "Jacking in From the 'Keys to the Kingdom' Port," *CyberWire Dispatch* (July 3, 1996)

The first evaluation of Cyber Patrol appeared in this early report on the problems of Internet filtering by journalists Brock Meeks and Declan McCullagh. They viewed a decrypted version of Cyber Patrol's block list (along with those of CYBERsitter and Net Nanny), and noticed that Cyber Patrol stored the Web addresses it blocked only partially, cutting off all but the first three characters at the end of a URL. For instance, the software was meant to block loiosh.andrew.cmu.edu/~shawn, a Carnegie Mellon student home page containing information on the occult; yet on its block list Cyber Patrol recorded only loiosh.andrew.cmu.edu/ ~sha, thereby blocking every site beginning with that URL segment and leaving, at the time of the report's publication, 23 unrelated sites on the university's server blocked.

The authors also found that with all default categories enabled, Cyber Patrol barred multiple sites concerning cyberliberties – the Electronic Frontier Foundation's censorship archive, for example, and MIT's League for Programming Freedom. Also blocked were the Queer Resources Directory, which counts among its resources information from the Centers for Disease Control and Prevention, the *AIDS Book Review Journal*, and *AIDS Treatment News*. Cyber Patrol also blocked a number of newsgroups dealing with homosexuality or gender issues, such as alt.journalism.gay-press; soc.support.youth.gay-lesbian-bi; alt.feminism; and soc.support.fat-acceptance.

Karen Schneider, *A Practical Guide to Internet Filters* (1997)

The Internet Filter Assessment Project tested Cyber Patrol configured to block only "full nudity" and "sexual acts." Schneider reported that the software "blocked "good sites" 5-10% of the time, and pornographic sites slipped through about 10% of the time. One of the "good sites" was www.disinfo.com, described by Schneider as a site "devoted to debunking propaganda."

Jonathan Wallace, "Cyber Patrol: The Friendly Censor" (Censorware Project, Nov. 22, 1997)

Jonathan Wallace tested approximately 270 sites on ethics, politics, and law – all "containing controversial speech but no obscenity or illegal material" – against the CyberNOT search engine after learning that the Web pages of *Sex, Laws, and Cyberspace*, the 1996 book he co-authored with Mark Mangan, were blocked by Cyber Patrol. Wallace found 12 of his chosen sites were barred, including *Deja News*, a searchable archive of Usenet materials, and the Society for the Promotion of Unconditional Relationships, an organization advocating monogamy. He could not find out which of Cyber Patrol's categories these sites fit into. When asked, a Cyber Patrol representative simply said that the company considered the sites "inappropriate for children."

Wallace reported that Cyber Patrol also blocked sites featuring politically loaded content, such as the Flag Burning Page, which examines the issue of flag burning from a constitutional perspective; Interactivism, which invites users to engage in political activism by corresponding with politicians on issues

[44] Cyber Patrol, "Accurate, Current & Relevant Filtering," www.cyberpatrol.com/Default.aspx?id=129&mnuid=2.5 (visited 2/26/06).

such as campaign finance reform and Tibetan independence; Newtwatch, a Democratic Party-funded page that consisted of reports and satires on the former Speaker of the House; Dr. Bonzo, which featured "satirical essays on religious matters"[45]; and the Second Amendment Foundation – though, as Wallace noted, Cyber Patrol did not block other gun-related sites, such as the National Rifle Association's.

Gay and Lesbian Alliance Against Defamation (GLAAD) press release, "Gay Sites Netted in Cyber Patrol Sting" (Dec. 19, 1997)

GLAAD reported that Cyber Patrol was blocking the entire "WestHollywood" subdirectory of Geocities. WestHollywood, at that time, was home to more than 20,000 gay- and lesbian-interest sites, including the National Black Lesbian and Gay Leadership Forum's Young Adult Program. When contacted, Cyber Patrol's then-manufacturer Microsystems Software cited, by way of explanation, the high potential for WestHollywood sites to contain nudity or pornographic imagery. GLAAD's press release pointed out, however, that Geocities expressly prohibited "nudity and pornographic material of any kind" on its server.

Microsystems CEO Dick Gorgens responded to further inquiry with the admission that GLAAD was "absolutely correct in [its] assessment that the subdirectory block on WestHollywood is prejudicial to the Gay and Lesbian Geocities community. ... Over the next week the problem will be corrected." Yet according to the press release, after a week had passed, the block on WestHollywood remained.

Censorware Project, *Blacklisted by Cyber Patrol: From Ada to Yoyo* (Dec. 22, 1997)

This report documented a number of sites that the Censorware Project considered wrongly blocked in the "full nudity" and "sexual acts" categories, among them Creature's Comfort Pet Service; Air Penny (a Nike site devoted to basketball player Penny Hardaway); the MIT Project on Mathematics and Computation; AAA Wholesale Nutrition; the National Academy of Clinical Biochemistry; the online edition of *Explore Underwater* magazine; the computer science department of England's Queen Mary and Westfield College; and the United States Army Corps of Engineers Construction Engineering Research Laboratories. The report took its title from two additional sites blocked for "full nudity" and "sexual acts": "We, the People of Ada," an Ada, Michigan, committee devoted to "bringing about a change for a more honest, fiscally responsible and knowledgeable township government," and Yoyo, a server of Melbourne, Australia's Monash University.

Blacklisted also reported that every site hosted by the free Web page provider Tripod was barred, not only for nudity or sexually explicit content, but also for "violence/profanity," "gross depictions," "intolerance," "satanic/cult," "drugs/drug culture," "militant/extreme," "questionable/illegal & gambling," and "alcohol & tobacco." Tripod was home, at the time of the report, to 1.4 million distinct pages, but smaller servers and service providers were also blocked in their entirety—*Blacklisted* lists 40 of them. Another section of the report lists hundreds of blocked newsgroups, including alt.atheism; alt.adoption; alt.censorship; alt.journalism; rec.games.bridge (for bridge enthusiasts); and support.soc.depression.misc (on depression and mood disorders).

The day after *Blacklisted* was published, Microsystems Software unblocked 55 of the 67 URLs and domains the report had cited. Eight of the remaining 12, according to the Censorware Project, were still wrongly blocked: Nike's Penny Hardaway site; the National Academy of Biochemistry sites;

[45] Wallace added that the blocking of this site, "long removed from the Web, raises questions about the frequency with which the Cyber Patrol database is updated."

four Internet service providers; Tripod; and a site-in-progress for a software company. This last site, at the time of Censorware's December 25, 1997 update to *Blacklisted,* contained very little content, but did contain the words "HOT WEB LINKS," which was "apparently enough for Cyber Patrol to continue to block it as pornography through a second review." Of the four other sites left blocked, two, Censorware acknowledged, fell within Cyber Patrol's blocking criteria and "shouldn't have been listed as wrongful blocks originally."[46]

Christopher Hunter, *Filtering the Future?: Software Filters, Porn, PICS, and the Internet Content Conundrum* (Master's thesis, Annenberg School for Communication, University of Pennsylvania, July 1999)

In June 1999, Christopher Hunter tested 200 URLs against Cyber Patrol and three other filters. Contending that existing reports on blocked sites applied "largely unscientific methods" (that is, they did not attempt to assess overall percentages of wrongly blocked sites), Hunter tested Cyber Patrol, CYBERsitter, Net Nanny, and SurfWatch by "social science methods of randomization and content analysis."

Hunter intended half of his testing sample to approximate an average Internet user's surfing habits. Thus, the first 100 sites consisted of 50 that were "randomly generated" by Webcrawler's random links feature and 50 others that Hunter compiled through AltaVista searches for the five most frequently requested search terms as of April 1999: "yahoo," "warez" (commercial software obtainable for download), "hotmail," "sex," and "MP3." Hunter gathered the first 10 matches from each of these five searches.

For the other 100 sites, Hunter focused on material often identified as controversial, such as the Web sites of the 36 plaintiff organizations in *ACLU v. Reno* and *ACLU v. Reno II*, the American Civil Liberties Union's challenges to the 1997 Communications Decency Act and 1998 Child Online Protection Act. Hunter then conducted Yahoo searches for sites pertaining to Internet portals, political issues, feminism, hate speech, gambling, religion, gay pride and homosexuality, alcohol, tobacco, and drugs, pornography, news, violent computer games, safe sex, and abortion. From each of the first 12 of these 13 searches, Hunter chose five of the resulting matches for his sample, and then selected four abortion-related sites (two pro- and two anti-) in order to arrive at a total of 100 URLs.

Hunter evaluated the first page of each site using the rating system devised by an industry group called the Recreational Software Advisory Council (RSAC). Under the RSAC's four categories (violence, nudity, sex, and language) and five grades within each category, a site with a rating of zero in the "sex" category, for example, would contain no sexual content or else only "innocent kissing; romance," while a site with a "sex" rating of 4 might contain "explicit sexual acts or sex crimes." Using these categories, Hunter made his own judgments as to whether a filtering product erroneously blocked or failed to block a site, characterizing a site whose highest RSAC rating he thought would be zero or one as nonobjectionable, while determining that any site with a rating of 2, 3, or 4 in at least one RSAC category should have been blocked.[47]

After testing each filter at its "default" setting, Hunter concluded that Cyber Patrol blocked 20 sites, or 55.6%, of the material he deemed objectionable according to RSAC

[46] Censorware Project, *Blacklisted By Cyber Patrol: From Ada to Yoyo – The Aftermath* (Dec. 25, 1997).

[47] Because the RSAC's system depended on self-rating, it never gained much traction in the U.S., where third-party filtering products soon dominated the market. In 1999, the RSAC merged with the Internet Content Rating Association (ICRA), a British-based industry group. See www.rsac.org; www.icra.org/about (both visited 3/14/05). For background on RSAC, ICRA, and their difficulty achieving wide acceptance, see Marjorie Heins, *Not in Front of the Children: "Indecency," Censorship, and the Innocence of Youth* (2001), 224, 261, 351-52.

standards, and 15 sites, or 9.1%, of the material he deemed innocuous. Among the 15 innocuous sites were the feminist literary group *RiotGrrl*; Stop Prisoner Rape; the Qworld contents page, a collection of links to online gay-interest resources; an article on "Promoting with Pride" on the Queer Living page; the Coalition for Positive Sexuality, which promotes "complete and honest sex education"; SIECUS, the Sexuality Information and Education Council of the United States; and Gay Wired Presents Wildcat Press, a page devoted to an award-winning independent press.

Although Hunter may well have been right that many of the blocked sites were relatively unobjectionable according to the RSAC ratings, Cyber Patrol's default settings for these filters (for example, "sex education") were specifically designed to sweep broadly across many useful sites. It's not entirely accurate, therefore, to conclude that the blocking of all these sites would be erroneous; rather, it would be the result of restrictive default settings and user failure to disable the pre-set categories. Five of the sites Hunter deemed overblocked by Cyber Patrol, for example, were alcohol- and tobacco-related, and thus fell squarely within the company's default filtering criteria.

In February 2000, filtering advocate David Burt (later to become an employee of N2H2) responded to Hunter's study with a press release citing potential sources of error.[48] Burt argued that "200 sites is far too small to adequately represent the breadth of the entire World Wide Web" and charged that all but the 50 randomly generated URLs constituted a skewed sample, containing content "instantly recognizable as likely to trigger filters" and "not represented in the sample proportionately to the entire Internet," thus giving rise to "much higher-than-normal error rates." A more serious problem, however, is that in attempting to arrive at "scientific" estimates of percentages of wrongly blocked sites, Hunter relied on his own subjective judgments on how the different Web sites fit into the RSAC's 20 separate rating categories.[49]

Center for Media Education (CME), *Youth Access to Alcohol and Tobacco Web Marketing: The Filtering and Rating Debate* (Oct. 1999)

The CME tested Cyber Patrol and five other filters for underinclusive blocking of alcohol and tobacco marketing materials. They first selected the official sites of 10 beer manufacturers and 10 liquor companies that are popular and "[have] elements that appeal to youth." They added 10 sites pertaining to alcohol – discussing drinking games or containing cocktail-making instructions, for example – and 14 sites promoting smoking. (As major U.S. cigarette brands are not advertised online, CME chose the home pages of such magazines as *Cigar Aficionado* and *Smoke*.) Cyber Patrol blocked only 43% of the promotional sites.

The CME also conducted Web searches on three popular search engines – Yahoo, Go/InfoSeek, and Excite – for the alcohol- and tobacco-related terms "beer," "Budweiser lizards," "cigarettes," "cigars," "drinking games," "home brewing," "Joe Camel," "liquor," and "mixed drinks." It then attempted to access the first five sites returned in each search. Cyber Patrol blocked 30% of the result pages, allowing, for example, cigarettes4u.com, tobaccotraders.com, and homebrewshop.com, which, according to the report, "not only promoted the use of alcohol and tobacco, but also sold products and accessories related to their consumption."

To test blocking of educational and public health information on alcohol and tobacco,

[48] Filtering Facts press release, "ALA Touts Filter Study Whose Own Author Calls Flawed" (Feb. 18, 2000).

[49] Hunter later testified as an expert witness for the plaintiffs in the lawsuit challenging CIPA. The district court noted that his attempt to calculate over- and underblocking rates scientifically, like a similar attempt by experts for the government, was flawed because neither began with a truly random sample of Web sites for testing. *American Library Ass'n v. U.S.*, 201 F. Supp. 2d at 437-38.

the CME added to its sample 10 sites relating to alcohol consumption – for instance, www.alcoholismhelp.com, Mothers Against Drunk Driving and the National Organization on Fetal Alcohol Syndrome, along with 10 anti-smoking sites, and the American Cancer Society. Cyber Patrol did not block any of the sites in this group. Nor did it block most sites returned by the three search engines when terms like "alcohol," "alcoholism," "fetal alcohol syndrome," "lung cancer," or "substance abuse" were entered. Cyber Patrol allowed access to an average of 4.8 of the top five search results in each case; CME deemed an average of 4.1 of these contained important educational information.

Eddy Jansson and Matthew Skala, *The Breaking of Cyber Patrol ®4* (Mar. 11, 2000)

Jansson and Skala decrypted Cyber Patrol's blacklist and found questionable blocking of Peacefire, as well as a number of anonymizer and foreign-language translation services, which the company blocked under all of its default categories. Blocked under every category but "sex education" was the Church of the SubGenius site, which parodies Christian churches as well as corporate and consumer culture.

Also on the block list, for "intolerance," were a personal home page on which the word "voodoo" appeared (in a mention of voodoocycles.com) and the Web archives of Declan McCullagh's Justice on Campus Project, which worked "to preserve free expression and due process at universities." Blocked in the "satanic/cults" category were Webdevils.com (a site of multimedia Net-art projects) and Mega's Metal Asylum, a page devoted to heavy metal music; the latter site was also branded "militant/extremist." Also blocked as "militant/extremist," as well as "violence/profanity" and "questionable/illegal & gambling," were a portion of the Nuclear Control Institute site; a personal page dedicated, in part, to raising awareness of neo-Nazi activity; multiple editorials opposing nuclear arms from Washington State's *Tri-City Herald*; part of the City of Hiroshima site; the former Web site of the American Airpower Heritage Museum in Midland, Texas; an Illinois Mathematics and Science Academy student's personal home page, which at the time of Jansson and Skala's report consisted only of the student's résumé; and the Web site of a sheet-music publisher.

The "Marston Family Home Page," a personal site, was also blocked under the "militant/extremist" and "questionable/illegal & gambling" categories – presumably, according to the report, because one of the children wrote, "This new law the Communications Decency Act totally defys [*sic*] all that the Constitution was. Fight the system, take the power back. ..."

Bennett Haselton, "Cyber Patrol Error Rate for First 1,000 .com Domains" (Peacefire, Oct. 23, 2000)

Haselton tested Cyber Patrol's average rate of error, using the same 1,000 dot-com domains as a sample that he used for an identical investigation of SurfWatch (see page 36). The CyberNOT list blocked 121 sites for portrayals of "partial nudity," "full nudity," or "sexual acts." Of these 121 sites, he eliminated 100 that were "under construction," and assessed the remaining 21. He considered 17 wrongly blocked, including a-actionhomeinspection.com; a-1bonded.com (a locksmith's site); a-1janitorial.com; a-1radiatorservice.com; and a-attorney-virginia.com. He deemed four sites appropriately blocked under Cyber Patrol's definition of sexually explicit content, for an error rate of 81%. Haselton wrote that Cyber Patrol's actual error rate was anywhere between 65-95%, but was unlikely to be "less than 60% across all domains," and as with Bess, that the results may have been skewed in Cyber Patrol's favor owing to the test's focus on dot-com domains, which "are more likely to contain commercial pornography than, say, .org domains."

Bennett Haselton & Jamie McCarthy, "Blind Ballots: Web Sites of U.S. Political Candidates Censored by Censorware" (Peacefire, Nov. 7, 2000)

In this Election Day report, Peacefire revealed that Cyber Patrol, configured to block "partial nudity," "full nudity," and "sexual acts," blocked the Web sites of four Republican candidates, four Democrats, and one Libertarian. The site of an additional Democratic candidate, Lloyd Doggett, was blocked under Cyber Patrol's "questionable/illegal/

Cyber Patrol, configured to block "partial nudity," "full nudity," and "sexual acts," blocked the Web sites of four Republican candidates, four Democrats, and one Libertarian.

gambling" category. The day after Peacefire published these findings, *ZDNet News* reporter Lisa Bowman contacted Cyber Patrol's then-manufacturer, SurfControl. A company spokesperson directed Bowman to the CyberNOT search engine, which indicated that none of the URLs was actually prohibited. But later the same day, after downloading Cyber Patrol's most recent block list, Bowman attempted to access each site, and found that the software did indeed bar her from the candidate sites in question.[50]

"Amnesty Intercepted: Global Human Rights Groups Blocked by Web Censoring Software" (Peacefire, Dec. 12, 2000)

"Amnesty Intercepted" reported the following organizations (among others) blocked by Cyber Patrol in the category of "sexually explicit" content: Amnesty International Israel; the Canadian Labour Congress; the American Kurdish Information Network, which tracks human rights violations against Kurds in Iran, Iraq, Syria, and Turkey; the Milarepa Fund, a Tibetan interest group; *Peace Magazine*; the Bonn International Center for Conversion, which promotes the transfer of human, industrial, and economic resources away from the defense sector; the Canada Asia Pacific Resource Network, whose stated mission "is to promote regional solidarity among trade unions and NGOs in the Asia Pacific" region; the Sisterhood Is Global Institute, an organization opposing violations of the human rights of women worldwide; the Metro Network for Social Justice; the Society for Peace, Unity, and Human Rights for Sri Lanka; and the International Coptic Congress.

"Digital Chaperones for Kids," *Consumer Reports* (Mar. 2001)

Consumer Reports found that Cyber Patrol failed to block 23% of the magazine's chosen 86 "easily located Web sites that contain sexually explicit content or violently graphic images, or that promote drugs, tobacco, crime, or bigotry." Yet it did block the home page of Operation Rescue (which the authors classified as objectionable on account of its graphic images of aborted fetuses). The filter also blocked such nonpornographic sites as Peacefire and Lesbian.org.

Kieren McCarthy, "Cyber Patrol Bans *The Register*," *The Register* (Mar. 5, 2001); Drew Cullen, "Cyber Patrol Unblocks *The Register*," *The Register* (Mar. 9, 2001)

Days after the *Consumer Reports* article appeared, the British newspaper *The Register* received word from an employee of Citrix Systems that he had been unable to access the *Register* from his office computer, on which the company had installed Cyber Patrol. SurfControl unblocked the site within days,

[50] Peacefire, "Inaccuracies in the 'CyberNOT Search Engine,'" (n.d.); Lisa Bowman, "Filtering Programs Block Candidate Sites," *ZDNet News* (Nov. 8, 2000).

with the exception of a page containing the December 12, 2000, article that was the basis of the initial block: a piece by *Register* staff reporter John Leyden on Peacefire's recently introduced filter-disabling program.[51]

A SurfControl representative explained: "*The Register* published an article written by Peacefire containing information on how to access inappropriate sites specifically blocked by Cyber Patrol. Given [the] irresponsible nature of the article, apparently encouraging users to override Cyber Patrol's filtering mechanism, we took the decision to block *The Register* – upholding our first obligation to customers by preventing children or pupils from being able to surf Web sites containing sexually explicit, racist or inflammatory material." Cullen responded that there was no "sexually explicit, racist," or "inflammatory" material in the article, which "merely describes peacefire.exe and provides a link to the Peacefire.org Web site."[52]

Miscellaneous reports

- In "Censorware: How Well Does Internet Filtering Software Protect Students?" (Jan. 1998), *Electronic School* columnist Lars Kongshem reported that Cyber Patrol blocked the "Educator's Home Page for Tobacco Use Prevention," part of a site maintained by Maryland's Department of Health and Mental Hygiene.
- In his expert witness report for the defendants in the case of *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library* (July 14, 1998), David Burt reported that his comparative testing of Cyber Patrol, I-Gear, SurfWatch, and X-Stop revealed that Cyber Patrol blocked 40% of sites Burt had selected as nonobscene, including the sex information sites *Di Que Si*; All About Sex; New Male Sexuality; and Internet Sex Radio.
- In the *New York Times* article "Library Grapples with Internet Freedom" (Oct. 15, 1998), Katie Hafner reported that Cyber Patrol blocked searches for Georgia O'Keeffe and Vincent van Gogh, while allowing hits from searches for "toys" that included sites selling sex toys.
- Peacefire reported, in "BabelFish Blocked by Censorware" (Feb. 27, 2001), that Cyber Patrol blocked the foreign-language Web page translation service featured on AltaVista in all 12 filtering categories.
- In "Teen Health Sites Praised in Article, Blocked by Censorware" (Mar. 23, 2001), Bennett Haselton reported that Cyber Patrol blocked ZapHealth, a health education site containing articles of interest to a teenage audience.

Cyber Sentinel

Rather than maintaining and updating a list of sites to be blocked, or designating forbidden categories, Cyber Sentinel scans each requested page for key words and phrases in its various databases, or "libraries." In 2001, for example, its "child predator library" contained such phrases and "do you have a pic" and "can I call you." Promotional text on Cyber Sentinel's Web site claims it is "the most advanced and flexible" Internet filtering product on the market.[53]

Center for Media Education, *Youth Access to Alcohol and Tobacco Web Marketing: The Filtering and Rating Debate* (Oct. 1999)

The CME found Cyber Sentinel ineffec-

[51] John Leyden, "Porn-filter Disabler Unleashed," *The Register* (Dec. 19, 2000).

[52] The SurfControl representative also wrote: "We should be grateful if *The Register* would adopt a policy of allowing companies, such as ourselves, the opportunity to respond in full before going to press." "Astonishing," Cullen commented. "Cyber Patrol blocked *The Register* without informing us, or giving us a chance to respond in full, or at all."

[53] "Cyber Sentinel Filtering Network," www.cyber-sentinel.net (visited 3/7/06). This site is operated by Software4Parents.com. Another product, "Cyber Sentinel Network," is made by Security Software Systems and seems to use similar technology, adjusted for office rather than home use, www.securitysoft.com/default.asp?pageid=49 (visited 3/7/06).

tive in screening out promotions for alcohol and tobacco use. It blocked only 11% of the promotional sites selected by the testers, allowing users to access an average of 39 of the 44 pages, and blocked just 3% of the pages resulting from searches for alcohol- and tobacco-related promotional material.

Bennett Haselton, "Sites Blocked by Cyber Sentinel" (Peacefire, Aug. 2, 2000)

Having conducted "about an hour of ad-hoc experimentation," Haselton found that Cyber Sentinel blocked CNN because, as system log files revealed, the word "erotic" appeared on the front page (in the title of an article, "Naples Museum Exposes Public to Ancient Erotica"). Also blocked were: a result page for a search of the word "censorship" on *Wired* magazine's site (one of the results contained the word "porn" in the title, "Feds Try Odd Anti-Porn Approach"); result pages for searches of the term "COPA" on *Wired* and other news sites, also on account of article titles containing the word "porn" (for instance, "Appeals Court Rules Against Net Porn Law"); and a portion of the Web site of the Ontario Center for Religious Tolerance, containing an essay on collisions between science and religion throughout history.

Cyber Sentinel also blocked sites associated with both sides of the civil liberties and Internet censorship debates: an ACLU press release, "Calls for Arrest of Openly Gay GOP Convention Speaker Reveal Danger of Sodomy Laws Nationwide"; the American Family Association, because of the word "porn" ("the current administration and the Justice Department have been good to the porn industry"); on account of the word "cum," the biographies of COPA Commission members Stephen Balkam and Donna Rice Hughes (both graduated *magna cum laude*); the COPA Commission's list of research papers, because the word "porn" appeared in the title of one report; and the home page for Donna Rice Hughes's book, *Kids Online: Protecting Your Children in Cyberspace*, an appendix of which is titled "Porn on the Net."

CYBERsitter

Before 1999, CYBERsitter, in addition to blocking entire sites and searches for terms on its block list, would excise terms it deemed objectionable and leave blank spaces where they would otherwise appear. This procedure led to some early notoriety for the product, as when it deleted the word "homosexual" from the sentence, "The Catholic Church opposes homosexual marriage" – and left Web users reading "The Catholic Church opposes marriage."[54]

In 1999, CYBERsitter, manufactured by Solid Oak Software, modified its system and established seven default settings, including "PICS rating adult topics," which covered "all topics not suitable for children under the age of 13," "sites promoting the gay and lesbian lifestyle," and "sites advocating illegal/radical activities." Its total list of blocking categories grew to 22. Users could enable or disable any category.

By 2005, CYBERsitter had 32 content categories, including "cults," "gambling," and "file sharing." Its default setting blocked "sex," "violence," "drugs," and "hate," as well as all image searches. *PC Magazine* called it "the strongest filtering we've seen. … CYBERsitter errs on the conservative side." It also blocked "bad words" in email and instant messages.[55]

Brock Meeks & Declan McCullagh, "Jacking in From the 'Keys to the Kingdom' Port," *CyberWire Dispatch* (July 3, 1996)

Meeks and McCullagh reported that CYBERsitter blocked a newsgroup devoted to gay issues (alt.politics.homosexual), the Queer Resources Directory, and the home page of the National Organization for Women. CYBERsitter's prohibited words included

[54] Peacefire, "CYBERsitter Examined" (2000).

[55] "CYBERsitter 9.0," *PC Magazine* (Aug. 3, 2004), www.pcmag.com/article2/0,1759,1618830,00.asp (visited 2/1/06); see also "CYBERsitter® – For a Family Friendly Internet," CYBERsitter.com (visited 2/10/06).

"gay, queer, bisexual" combined with "male, men, boy, group, rights, community, activities…" and "gay, queer, homosexual, lesbian, bisexual" combined with "society, culture."

According to the report, Brian Milburn, president of Solid Oak Software, responded: "We have not and will not bow to pressure from any organization that disagrees with our philosophy. ... We don't simply block pornography. That's not the intention of our product. The majority of our customers are strong family-oriented people with traditional family values. ... I wouldn't even care to debate if gay and lesbian issues are suitable for teenagers. … We filter anything that has to do with sex. Sexual orientation [is about sex] by virtue of the fact that it has sex in the name."

Bennett Haselton, "CYBERsitter: Where Do We Not Want You To Go Today?", *Ethical Spectacle* (Nov. 5-Dec. 11, 1996)

Haselton reported that among CYBERsitter's blocked domains were, in addition to Peacefire itself, the online communities Echo Communications and Whole Earth 'Lectronic Link; the Web site of Community ConneXion, which manufactured an anonymous-surfing program; and the home page of the National Organization for Women. CYBERsitter also barred any Yahoo search for the term "gay rights."

Ethical Spectacle press release, "CYBERsitter Blocks *The Ethical Spectacle*" (Jan. 19, 1997)

In early 1997, CYBERsitter blocked the *Ethical Spectacle*, an online magazine "examining the intersection of ethics, law and politics in our society," after editor Jonathan Wallace added a link to a site titled "Don't Buy CYBERsitter," which directed users to Peacefire's report "CYBERsitter: Where Do We Not Want You to Go Today?" Wallace wrote to Milburn and Solid Oak technical support "demanding an explanation. I pointed out that *The Spectacle* does not fit any of their published criteria for blocking a site. I received mail in return demanding that I cease writing to them and calling my mail 'harassment' —with a copy to the postmaster at my ISP."

Karen Schneider, *A Practical Guide to Internet Filters* (1997)

Schneider's Internet Filter Assessment Project reported that unlike other filtering products, CYBERsitter does not permit its keyword-blocking feature to be disabled. Regarding CYBERsitter's claim that it "looks at how the word or phrase is used in context," Schneider quoted one TIFAP tester: "Nothing could be further from the truth." The filter deleted the word "queer," for example, from Robert Frost's "Stopping by Woods on a Snowy Evening" ("My little horse must think it queer / To stop without a farmhouse near"). CYBERsitter did not block sites containing instructions for growing marijuana, but did block a news item on the legislation surrounding it.

Marie José Klaver, "What Does CYBERsitter Block?" (June 23, 1998)

In June 1998, Marie-José Klaver decrypted and published CYBERsitter's full list of blocked words, strings, sites, and domains. Among the domains on the block list were servers of the University of Chicago, the University of Virginia's Information Technology & Communication Division, Georgia State University, the University of Michigan's engineering department, and Rutgers University; several large Dutch domains, including euronet.nl, huizen.dds.nl, and worldaccess.nl; and the phrases "bennetthaselton," "peacefire," and "dontbuyCYBERsitter."

Christopher Hunter, *Filtering the Future* (July 1999)

Though Christopher Hunter's study (see page 17) concluded that CYBERsitter was the most reliable filter at screening out "objectionable" sites (it blocked 25, or 69.4%, of such sites in his sample), he also noted that the

software performed well below the 90-95% rate of accuracy boasted by the manufacturer. CYBERsitter fared worst in its treatment of "nonobjectionable" material, blocking 24, or 14.6%, of the sites to which Hunter assigned RSAC ratings no higher than one. Among these were *Sharktagger*, a site promoting responsible shark fishing and conservation; a listing of local events posted on Yahoo; *RiotGrrl*; Planned Parenthood; Stop Prisoner Rape; the National Organization for Women; the feminist performance-art and activist troupe Guerrilla Girls; the Church of Scientology; The Body, an informational site on AIDS and HIV; Williams College's information page on safe sex; the Coalition for Positive Sexuality, SIECUS, and Pro-Life America.

Cybersitter left Web users reading "the Catholic Church opposes marriage."

CYBERsitter proved particularly likely to deny access to nonpornographic sites relating to homosexuality, blocking the QWorld contents page; the gay communities Planet Out, PrideNet, and the Queer Zone; A Different Light Bookstore, which specializes in gay and lesbian literature; Gay Wired Presents Wildcat Press; and Queer Living's "Promoting with Pride" page. (These sites, while not falling under RSAC's definition of unacceptability, do fall within CYBERsitter's default filtering category of "sites promoting the gay and lesbian lifestyle.")

Center for Media Education, *Youth Access to Alcohol and Tobacco Web Marketing* (Oct. 1999)

The CME charged CYBERsitter with under- and overinclusive filtering of alcohol- and tobacco-related material, as it blocked only 19% of the promotional sites in the test sample – leaving unblocked beer sites such as heineken.com, and sites on which tobacco products were sold, such as lylessmokeshop .com. While performing better than most other filters in its response to searches for promotional content – CYBERsitter prohibited searches for "beer," "cigarettes," "cigars," and "liquor" – it subsequently blocked just 3% of the result pages (from the allowed searches) that the CME testers attempted to view. CYBERsitter also blocked 13% of the CME's chosen educational and public health sites, and prohibited testers from conducting searches for "alcohol," "alcoholism," "fetal alcohol syndrome," "tobacco," and "tobacco settlement."

Peacefire, "CYBERsitter Examined" (2000)

The original report on this study described CYBERsitter's blocking of numerous nonprofit sites, including the Penal Lexicon, a British project documenting prison conditions worldwide; the Department of Astronomy at Smith College; the Computer Animation Laboratory at the California Institute of the Arts; and the College of Humanities & Social Sciences at Carnegie Mellon University. The filter's by-then well-known propensity for overblocking resulted from its keyword-based technology, combined with the manufacturer's decision to block sites like the National Organization for Women in order to appeal to a rightwing constituency. The current text of "CYBERsitter Examined" recounts the history of CYBERsitter's disputes with its critics, and links to lists of previously blocked sites.

Bennett Haselton, "Amnesty Intercepted: Global Human Rights Groups Blocked by Web Censoring Software" (Peacefire, Dec. 12, 2000)

CYBERsitter blocked a number of pages on the Amnesty International site because of its keyword filtering mechanism. A news item containing the sentence, "Reports of shootings in Irian Jaya bring to at least 21 the number of people in Indonesia and East Timor killed or wounded," was prohibited for its "sexually explicit" content. Peacefire's review

of the system log revealed that CYBERsitter had blocked the site after detecting the words "least 21." The filter blocked another human rights page, which noted that the United Nations Convention on the Rights of the Child "defines all individuals below the age of 18 years as children," for the words "age of 18."

"Digital Chaperones for Kids," *Consumer Reports* (Mar. 2001)

While failing to block 22% of sites that *Consumer Reports* deemed objectionable because of "sexually explicit content or violently graphic images" or promotion of "drugs, tobacco, crime, or bigotry," CYBERsitter blocked nearly one in five of the sites the authors considered inoffensive, including Lesbian.org, the Citizens' Committee for the Right to Keep and Bear Arms, and the Southern Poverty Law Center.

Miscellaneous reports

- In a review of "Filtering Utilities" (Apr. 8, 1997), *PC Magazine* noted that CYBERsitter blocked an engineering site with "BourbonStreet" in its URL.
- According to the Digital Freedom Network's "Winners of the Foil the Filter Contest" (Sept. 28, 2000), CYBERsitter blocked House Majority Leader Richard "Dick" Armey's official Web site upon detecting the word "dick," and Focus on the Family's Pure Intimacy page, which protests pornography and is geared toward individuals "struggling with sexual temptations."
- In "Teen Health Sites Praised in Article, Blocked by Censorware" (Mar. 23, 2001), Peacefire's Bennett Haselton reported that CYBERsitter barred part or all of three out of the four sites discussed in a recent *New York Times* article on health education resources for teenagers: ZapHealth; various pages on Kidshealth.org, including its anti-smoking page, a page of advice on travel safety, and a profile of KidsHealth staff member Pamela Arn – presumably because CYBERsitter detected its blacklisted phrase "pamela.html" in the URL and confused the site with one devoted to Pamela Anderson; and part of iEmily.com, including the Terms of Service page, on which the words "sexually oriented" appeared. (One of the terms of service is that users "will not use [iEmily's] message boards or chat rooms to post any material which is ... sexually oriented.")
- In a Censorware Project post, "Columnist Opines Against Censorware, Gets Column Blocked" (Mar. 29, 2001), Bennett Haselton reported that CYBERsitter blocked "Web Filters Backfire on their Fans," a *Chicago Tribune* article that criticized filtering software, apparently because the software detected the words "porno," "Internet porn," and "Peacefire" in the article.
- A short article by Greg Lindsay in *Time Digital* (Aug. 8, 1997), referenced by Peacefire's "Blocking Software FAQ" reported that CYBERsitter blocked a *Time* magazine article critical of the filter.

FamilyClick

FamilyClick, whose spokesperson was anti-pornography activist Donna Rice Hughes, allowed users to choose from five configurations. Its least restrictive "Full FamilyClick Access" setting, recommended for ages 18+, blocked sites falling into any of seven categories, including "crime," "gambling," and "chat." Its "Teen Access" setting, for ages 15-17, blocked the previous seven categories plus "personals," "illegal drug promotion," "chat/message boards," and "non-FamilyClick email services." "Preteen Access," for ages 12-14, barred four additional categories, including "advanced sex education" and "weapons." "Kids Access," geared toward ages 8-11, blocked "basic sex education." Finally, the "Children's Playroom," for ages seven and under, was described as "100% safe. It

contains activities, games and content that have been pre-selected and pre-approved by FamilyClick."

The filter's Web site in 2005 stated that "FamilyClick has ceased operating its filtering service until further notice."[56]

Bennett Haselton, "Sites blocked by FamilyClick" (Peacefire, Aug. 1, 2000)

Haselton conducted "about an hour's worth of ad-hoc testing" of FamilyClick on its least restrictive "18+" setting and found that among the sites blocked were: a report from the U.S. embassy in Beijing on the AIDS epidemic in China; a research study on gambling in Washington State; a Spanish-language glossary of AIDS terms; the home page of Camp Sussex, which organizes summer programs for children of low-income households; *Psyart*, an online journal published by the University of Florida's Institute for the Psychological Study of the Arts; an essay titled "Triangles and Tribulations: The Politics of Nazi Symbols," on a Holocaust Studies site; a *Christian Research Journal* article condemning homosexuality; and the genealogical page for one Alice Ficken – perhaps, Haselton observed, because "Ficken" is the infinitive form of "fuck" in German.

I-Gear barred searches on eating disorders, AIDS, and child labor.

Other blocked sites included an inventory of state sodomy laws on the Web site of the ACLU; a genealogical index of individuals bearing the name "Mumma"; a background report on pornography by the Minnesota Family Council; a page on the Ontario Center for Religious Tolerance site that tracked anti-Wiccan content on Christian Web sites; an essay on the Federation of American Scientists site called "Countering Terrorism," regarding the slaying of 11 Israeli athletes at the 1972 Munich Olympics; and a guide to "Eating Right" for chronic obstructive pulmonary disease patients.

Online Policy Group, "Online Oddities and Atrocities Museum" (n.d.)

The Online Policy Group maintained, as part of its "Online Oddities and Atrocities Museum," a list of sites at different times mistakenly blocked by FamilyClick. These included the Christian Coalition (which is headed by FamilyClick founder Tim Robertson's father, Pat Robertson), The Oprah Winfrey Show, which was blocked, in the midst of a product demonstration by Donna Rice Hughes during her appearance on that program; and the FamilyClick site itself.

I-Gear

I-Gear, manufactured by the Symantec Corporation, as of 2001 operated through a combination of predefined URL databases and "Dynamic Document Review." As it described the process, I-Gear divided its site database into 22 categories. If a URL was not in any of the databases, I-Gear scanned the page for trigger words from its "DDR Dictionaries." Each matching word on a site received a numerical score; if the total score for the page exceeded 50 (the default maximum score, which could be adjusted to anywhere between 1-200), the site was blocked.

By 2005, Symantec had reconfigured I-Gear to be a component of larger products such as "Symantec Web Security," which combines filtering out "inappropriate" content with anti-virus and other noncensorship-based protections.[57] We were unable to find any description of the filtering method used, beyond the assurance that Symantec Web Security "ensures maximum protection by combining

[56] Family Click: Your Guide to the Web," www.familyclick.com (visited 3/13/05).

[57] "Symantec Web Security," enterprisesecurity.symantec.com/products/products.cfm?ProductID=60 (visited 3/14/05).

list-based techniques with heuristic, context-sensitive analysis tools."[58]

Karen Schneider, *A Practical Guide to Internet Filters* (1997)

Schneider suggested that I-Gear's state-of-the-art-sounding Dynamic Document Review basically amounted to keyword blocking. For this reason, TIFAP tested I-Gear under its least restrictive "adult" setting with DDR disabled, thus using only the list of proscribed URLs. It found that, even with this configuration, I-Gear blocked the entire Gay and Lesbian directory of Yahoo, as well as pages containing the words "cockfighting" and "pussycat."

Anemona Hartocollis, "Board Blocks Student Access to Web Sites: Computer Filter Hobbles Internet Research Work," *New York Times* (Nov. 10, 1999)

The *New York Times* reported that I-Gear barred students at Benjamin Cardozo High School in New York City from conducting searches on such topics as breast cancer, eating disorders, AIDS, and child labor. Though Symantec senior product manager Bernard May responded to the news by insisting that I-Gear demonstrated "absolutely no preference of one group or another," the article also noted that I-Gear blocked the pro-choice groups Planned Parenthood and Alan Guttmacher Institute, but not Right to Life and Operation Rescue. Students were also unable to access portions of an electronic text of *The Grapes of Wrath* – specifically, "a passage in which a woman lets a starving man suckle at her breast."

Peacefire, "Analysis of First 50 URLs Blocked by I-Gear in the .edu Domain" (Mar. 2000)

Peacefire evaluated the first 50 dot-edu sites blocked in the "sexual acts" category according to a February 2000 I-Gear block list. Of the 50 blocks, Peacefire determined that 27 were "obvious errors" and 10, "marginal errors" (blocking of sites with moderately adult content but not falling within I-Gear's definition of "sexual acts"). Among the "obvious" wrongful blocks were sites containing references to or information on homosexuality, such as the personal home page of Carnegie Mellon Robotics Institute programmer Duane T. Williams and an anti-gay pamphlet, posted on the Web site of the Gay and Lesbian Alliance at the Georgia Institute of Technology. Also blocked were sites with anti-censorship content; astronomy, cartography, and art museum sites; and an essay on "Indecency on the Internet: Lessons from the Art World," by Julie Van Camp, a philosophy professor at the University of California.

Other sites blocked for reasons unknown included "Semi-Automatic Morph Between Two Supermodels," an animation sequence written by an MIT student in which images of two models' faces morph into each other; a diagram of a milk pasteurization system; a site containing Book X, in Latin, of the *Confessions* of St. Augustine – possibly because of the common appearance of the word "cum";[59] two pages on the Wheaton College server containing sections of *The Decline and Fall of the Roman Empire*; and lecture notes from a philosophy course at the University of Notre Dame.

Peacefire, "I-Gear Examined" (2000)

In tests of I-Gear throughout the first half of 2000, Peacefire found more sites blocked for questionable reasons, including the full text of *Jane Eyre*; the federal district court's ruling on the Communications Decency Act in *ACLU v. Reno*; transcripts of testimony from *ACLU v. Reno*; "Readings on Computer Communications and Freedom of Expression," a supplementary reading list for a course on Internet ethics at MIT; and the free speech page of the Center for Democracy and Technology.

[58] "Symantec Web Security," eval.veritas.com/mktginfo/enterprise/fact_sheets/ent-factsheet_web_security_3.0_05-2005.en-us.pdf (visited 3/2/06).

[59] Chris Oakes, "Censorware Exposed Again," *Wired News* (Mar. 9, 2000)

I-Gear also barred a United Nations report, "HIV/AIDS: The Global Epidemic"; the Albert Kennedy Trust, which works on behalf of homeless gay teenagers; the Anti-Violence Project, which opposes anti-gay violence; the International Gay and Lesbian Human Rights Committee; the Human Rights Campaign; the Harvard Gay and Lesbian Caucus; two pages of the National Organization for Women site, one providing information on gay rights, the other a press release on the legal status of gay marriage in Hawaii; a statement on equal rights for homosexuals and women in the workplace from the Industrial Workers of the World; a portion of GLAAD's site containing information for prospective volunteers; "The Homosexual Movement: A Response," a statement by a group of Jewish and Christian theologians, ethicists, and scholars; two Web sites relating to the Christian Coalition – the organization's legal arm, the American Center for Law and Justice, and the Pat Robertson-owned Christian Broadcasting Network; and the home page of the British Conservative Party.

Other blocked sites included a Cato Institute policy paper titled "Feminist Jurisprudence: Equal Rights or Neo-Paternalism?"; a gender studies page on Carnegie Mellon University's English server; Planned Parenthood; CyberNOTHING's critical commentary on a 1995 *Time* magazine cover story about pornography online; and the article "PETA and a Pornographic Culture," which protested the use of nude models in recent PETA advertising campaigns, but contained no nude images. Peacefire does not indicate which I-Gear categories were enabled when the various sites were blocked.

Miscellaneous reports

- In his July 1998 expert witness report for the defendants in *Mainstream Loudoun v. Board of Trustees of Loudoun County Library*, David Burt reported that I-Gear blocked the Born-Again Virgins site; the Fine Art Nude Webring; and the home pages of four fine art photography galleries.
- Peacefire's "Amnesty Intercepted" (Dec. 12, 2000) reported that I-Gear blocked the official site of the 1999 International Conference Combating Child Pornography on the Internet.
- In the March 23, 2001 report "Teen Health Sites Praised in Article, Blocked by Censorware," Bennett Haselton reported that I-Gear's Dynamic Document Review led to the partial blocking of three sites lauded in a recent *New York Times* article describing health education sites for teens: iEmily; KidsHealth; and ZapHealth.

Internet Guard Dog

Internet Guard Dog, manufactured by McAfee, claimed in 2001 that it had "a comprehensive objectionable content database" that prevented "messages deemed inappropriate … from reaching your child." "Offensive words" as well as sites were blocked. A June 9, 2000 review noted that Guard Dog allowed the user to filter by category (*e.g.*, drugs, gambling, the occult) from levels 0 through 4, and that "when a line contains a disallowed word, Guard Dog replaces the entire line with asterisks."[60] By 2005, McAfee was no longer marketing Internet Guard Dog, but instead offered "McAfee Parental Controls"; we could find no information about blocking categories.[61]

---

[60] Review of Internet Guard Dog, *ZdNet* (June 9, 2000), URL no longer available. A March search found a *ZdNet* page noting that Guard Dog 3.0 "is not yet available from any of our online merchants." "Guard Dog 3.0 Win 9X," shopper-zdnet.com.com/Guard_Dog_3_0_Win9X/4027-3666_15-1587666.html?tag=search&part=&subj= (visited 3/10/06).

[61] us.mcafee.com/root/package.asp?pkgid=146&WWW_URL=www.mcafee.com/myapps/pc/default.asp (visited 3/13/05). By 2006, this URL led to a different site, advertising McAfee Privacy Service," us.mcafee.com/root/package.asp?pkgid=146&WWW_URL=www.mcafee.com/myapps/pc/default.asp (visited 3/10/06).

"Digital Chaperones for Kids," *Consumer Reports* (Mar. 2001)

Guard Dog failed to block 30% of "easily located Web sites that contain sexually explicit content or violently graphic images, or that promote drugs, tobacco, crime, or bigotry." It did block nearly 20% of sites that the testers deemed politically controversial but not pornographic or violent, including the National Institute on Drug Abuse and *SEX, Etc.*, the Rutgers University educational site written by and for teens.

Net Nanny

Net Nanny advertises itself as "the Web's original Internet filter," first launched in January 1994.[62] It is a freestanding software product that blocks based on "known inappropriate key words and phrases" and, as of 2005, on a monthly updated block list. Customers can customize their block lists, filter settings, and keyword lists.[63] As of 2006, Net Nanny had five blocking categories: "sexual explicitness," "hate," "violence," "crime," and "drugs."

While generally commended for its willingness to disclose its lists, Net Nanny has nonetheless fared poorly in studies, with high rates of both over- and underblocking.

Karen Schneider, *A Practical Guide to Internet Filters* (1997)

Schneider reported that Net Nanny blocked a long-obsolete URL containing artistic erotica, which was part of an early version of Yahoo, but did not block www.creampie.com, a sexually explicit site that had been in existence for six months.

Christopher Hunter, *Filtering the Future* (July 1999)

Hunter concluded, based on his designations of objectionable and nonobjectionable sites (see page 17), that Net Nanny's major failing lay in its underinclusive blocking. The software "performed horrendously," he wrote, "blocking a measly 17% of objectionable content" (it failed to block 30 sites, including www.xxxhardcore.com and www.ultravixen.com). But it also blocked the fewest "nonobjectionable sites" (3%). That 3% consisted of the Queer Resources Directory; the official home page of the White House; the Web site of Northwestern University professor and Holocaust revisionist Arthur Butz; the Adelaide Institute, another revisionist history site; an online casino; and the Coalition for Positive Sexuality.

Center for Media Education, *Youth Access to Alcohol and Tobacco Web Marketing* (Oct. 1999)

Net Nanny allowed every search that the CME attempted, for both promotional and educational alcohol- and tobacco-related sites. It blocked just 2% of the promotional sites in the test sample. Though initially unable to access the Cuervo Tequila site, CME researchers easily viewed it by entering the page's numerical IP address instead of its alphabetical one. Thus, "it would appear that Net Nanny does not regularly take IP addresses into consideration when compiling its blacklist" – making it easy to circumvent. What Net Nanny did block was health.org, apparently because its front page title, "Drug AbuseXXXXXXXXXX," was detected by the product's keyword-blocking feature.

Peacefire, "Net Nanny Examined" (2000)

Among the newsgroups that Peacefire found inappropriately blocked by Net Nanny were bit.listserv.aidsnews; sci.med.aids; and alt.feminism. Other blocked sites included the Banned Books page at Carnegie Mellon University and Femina.com, a "comprehensive, searchable directory of links to female friendly sites and information." Peacefire observed that

[62] "Net Nanny is CIPA-Compliant and More," www.netnanny.com/p/page?sb=cipa (visited 2/22/06).

[63] "Find Out More About Net Nanny," www.netnanny.com/page?sb=detailed, and www.netnanny.com/NetNanny5/assets/docs/nn5/userguide.pdf (visited 2/22/06).

"while the Banned Books page and Femina.com are blocked because the URLs exist as entries on Net Nanny's blocked site list, more Web sites are blocked because they contain keywords which activate Net Nanny's word filter."

"Digital Chaperones for Kids," *Consumer Reports* (Mar. 2001)

Consumer Reports reinforced Hunter's and the CME"s conclusions, reporting that Net Nanny failed to block 52% of 86 "easily located Web sites" selected by the magazine that "contain sexually explicit content or violently graphic images, or that promote drugs, tobacco, crime, or bigotry." The filter did, however, block Rutgers University's teen-oriented *SEX, Etc*.

Miscellaneous reports

- According to Brock Meeks and Declan McCullagh's "Jacking in From the 'Keys to the Kingdom' Port" (July 3, 1996), Net Nanny blocked every mailing list originating at cs.coloradu.edu, the computer science division of the University of Colorado, as well as unspecified "feminist newsgroups."
- In "Adam and Eve Get Caught in 'Net Filter" (Feb. 5, 1998), the *Wichita Eagle* reported that students at Wichita's Friends University, where Net Nanny had been installed at public computer stations, were barred from accessing pages containing educational material on sexually transmitted diseases, prostitution, and Adam and Eve.
- Net Nanny was cited in the Digital Freedom Network's "Winners of the Foil the Filter Contest" (Sept. 28, 2000) for blocking House Majority Leader Richard "Dick" Armey's official Web site upon detecting the word "dick." It also precluded a high school student in Australia from accessing sites on the genetics of cucumbers once Net Nanny detected the word "cum" in "cucumbers."

Net Shepherd

In October 1997, the AltaVista search engine and the organization Net Shepherd launched a "Family Search" function to screen the results of AltaVista searches according to NetShepherd's database of site ratings. Net Shepherd claimed to have rated more than 300,000 sites based on "quality" and "maturity," relying on "demographically appropriate Internet users'" judgments of what would be "superfluous and/or objectionable to the average family."[64]

By 2005, Net Shepherd seemed to be out of business. The original URLs for the product led to alternative sites, and a "Net Shepherd World Opinion Rating" site describing the software had not been updated since November 1997.[65]

Electronic Privacy Information Center (EPIC), *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet* (1997)

In November 1997, EPIC performed the same 100 searches on standard AltaVista and the "Family Search" version. Its sample of search terms included 25 schools, 25 charitable and political organizations, 25 educational and cultural organizations, and 25 "miscellaneous concepts and entities" that could be of research interest to children, for instance "astronomy," "Bill of Rights," "Teen Pregnancy," and "Thomas Edison."

The first search term on EPIC's list was "Arbor Heights Elementary." This primary school's site contained, among other features, an online version of *Cool Writers Magazine*, a literary periodical for ages 7-12. The search on unfiltered AltaVista resulted in 824 sites mentioning the school, while the same search through Net Shepherd returned only three.

[64] Net Shepherd press release (Dec. 1997).

[65] "Net Shepherd World Opinion Rating Service," www.research.att.com/projects/tech4kids/Net_Shepherd_World_Opinion_Rating_Service.html (visited 3/13/05; 2/26/06).

Thus, EPIC determined that 99.6% of search results were filtered out. In subsequent searches for elementary, middle, and high schools, EPIC concluded that Net Shepherd blocked between 86-99% of relevant material.

EPIC found similar filtering of information about charitable and political organizations, ranging from 89-99.9%. Among the most heavily filtered search results were those for "American Cancer Society" (which had 38,762 relevant sites on an unfiltered search but only six with Net Shepherd), "United Jewish Appeal" (for which Net Shepherd allowed only one of the 3,024 sites that were otherwise reported as relevant); and "United Way" (for which Net Shepherd allowed 23 out of 54,300 responsive sites). Net Shepherd also filtered between 91-99.9% of relevant educational, artistic, and cultural institutions. On a search for "National Aquarium," it allowed 63 of the 2,134 sites otherwise reported by AltaVista. Similarly, it blocked 99.5% of sites responsive to the search term "photosynthesis," 99.9% for "astronomy," and 99.9% for "Wolfgang Amadeus Mozart."

The authors note some limitations in this study, including the fact that the blocking percentages could be lower than reported because even unfiltered AltaVista would not have provided access to all the responsive sites. Nevertheless, the obvious inference from this study is that Net Shepherd was filtering out all of the Internet except for a relative handful of approved, or "whitelisted," sites.

Norton Internet Security Family Edition (NIS)

The Norton Internet Security Family Edition is manufactured by Symantec, which also produces I-Gear (now embedded in Symantec Web Security). The methodology and blocking categories are the same as I-Gear's. As of 2005, the program had 31 categories of disapproved content. There was no override function allowing users to unblock mistakenly blocked sites.[66]

"Digital Chaperones for Kids," *Consumer Reports* (Mar. 2001)

Consumer Reports found that the NIS Family Edition left unblocked 20% of the sites the magazine deemed objectionable, while blocking such organizations as the Citizens' Committee for the Right to Keep and Bear Arms and the National Institute on Drug Abuse.

SafeServer

As of 2005, SafeServer relied on "Intelligent Content Recognition Technology," which it described as "a leading-edge technology based on artificial intelligence and pattern recognition ... trained to detect English-language pornography" and to screen requested Web pages in real time. Hence, its advertisement: "No lists, no subscriptions. Just fast, reliable filtering." It had seven categories of blockable content: "hate," "pornography," "gambling," "weapons," "drugs," "job search," and "stock trading."[67]

Bennett Haselton, "SafeServer Error Rate for First 1,000 .com Domains" (Peacefire, Oct. 23, 2000)

On a SafeServer proxy in use at a high school where a student had volunteered to assist with the research, Peacefire attempted to access a selection of commercial domains used earlier in an identical test of SurfWatch, and also in concurrent tests of Cyber Patrol and AOL Parental Controls. SafeServer was configured to bar the categories of "drugs," "gambling," "hate," "pornography," and "weapons." The filter blocked 44 pages in the 1,000-site sample; 15 of those 44 were "under construction." Haselton determined that of

[66] "TopTen Reviews," internet-filter-review.toptenreviews.com/ (visited 7/21/05); "Norton Internet Security," www.symantec.com/home_homeoffice/products/internet_security/nis-30mac/features.html (visited 2/27/06).

[67] "Foolproof SafeServer," smartstuff.com/safeserver/fepsafeserv.html; "Frequently Asked Questions," smartstuff.com/safeserver/fpserverfaq.html (both visited 7/21/05).

the remaining 29 sites, 10 were inappropriately blocked: a-1autowrecking.com; a-1coffee.com; a-1security.com; a-1upgrades.com; a-2-r.com; a-abacomputers.com; a-artisticimages.com; a-baby.com; a-build.com; and a-c-r.com. As with other filters tested, Haselton acknowledged that the resulting error rate of 34% was not entirely reliable because of the small sample under review, and that SafeServer could have an error rate as low as 15%; but that the rate of error among .org sites would presumably be higher, since pornographic sites were more prevalent among commercial domains.

SafeSurf

SafeSurf operates a voluntary self-rating system. Authors of Web pages can evaluate their sites according to 10 content categories, including "profanity," "nudity," "glorifying drug use," and "other adult themes." In addition, each page is assigned a numerical rating, or a "SafeSurf Identification Standard" from 1-9. Web publishers may assign themselves ratings in other categories as necessary – for example, a "nudity" rating of one if the site includes "subtle innuendo; [nudity] subtly implied through the use of composition, lighting, shaping, revealing clothing, etc.," or a rating of seven if it presents "erotic frontal nudity."

In 1996, SafeSurf and 22 other companies founded the Platform for Internet Content Selection (PICS). After Web publishers rate their sites, PICS-compliant software can read the ratings and filter accordingly. SafeSurf's filter "is a server solution, which means that the software is not installed at the end user's computer, but at the ISP level to avoid tampering."[68]

Peacefire, "SafeSurf Examined" (2000)

SafeSurf blocked multiple sites containing opposition to Web censorship and filtering, including: the Electronic Frontier Foundation's Internet Censorship and Regulation archive; a list of free speech links on the Web site of the American Communication Association; "The X-Stop Files" and "The Mind of a Censor," two articles in *The Ethical Spectacle*; a *CNet news* article on guidelines drafted by the American Library Association for countering campaigns for mandatory filtering ; the Wisconsin Civil Liberties Union and the National Coalition Against Censorship; and a *Scientific American* article on "Turf Wars in Cyberspace." SafeSurf also blocked the online edition of *Free Inquiry*, a publication of the Council for Secular Humanism; a United Nations paper on "HIV/AIDS: The Global Epidemic"; and the full texts of *The Odyssey* and *The Iliad*, both of which appeared on the University of Oregon server. Since it is unlikely that any of these sites self-rated, the probable explanation for the blocks is that SafeSurf filtered out all unrated sites.

SmartFilter

SmartFilter, manufactured by Secure Computing, was originally intended for companies seeking to limit their employees' non-work-related Internet usage. By 1999, it was also targeting schools.[69] The filter's control list has been modified, but on the whole, prior to 2001 SmartFilter divided objectionable sites into 27 categories, which could be enabled according to each customer's needs. When SmartFilter 3.0 was unveiled in January 2001, three of the categories ("alternative journals," "non-essential," and "worthless") had been removed, and six others added, including "mature" and "nudity."

In 2003, Secure Computing acquired N2H2, and their databases were merged. In 2006, the SmartFilter Control List contained

[68] "Just the FAQs Please," www.safesurf.com/ssfaq.htm (visited 3/10/06); see also "Microsoft Teams With Recreational Software Advisory Council To Pioneer Parental Control Over Internet Access," www.w3.org/PICS/960228/Microsoft.html (visited 2/26/06).

[69] Secure Computing, "Education and the Internet: A Balanced Approach of Awareness, Policy, and Security" (1999), www.netapp.com/ftp/internet_and_education.pdf (visited 3/14/05).

73 content-based categories. The company says that it uses "a combination of advanced technology and highly skilled Web analysts" to identify sites for blocking.[70]

Karen Schneider, *A Practical Guide to Internet Filters* (1997)

Testing SmartFilter with only its "sex" category enabled, TIFAP found 12 sites blocked – seven of them erroneously, in TIFAP's estimation. These included three sites on marijuana use, three gay-interest sites, and a site containing safe sex information.

Peacefire, "SmartFilter Examined" (1997)

Peacefire tested SmartFilter configured to block sites falling into categories likely to be activated in a school setting: "criminal skills," "drugs," "gambling," "hate speech," and "sex." Among the sites blocked were: Community United Against Violence, which works to prevent anti-gay hate crime; Peaceable Texans for Firearms Rights; the Marijuana Policy Project; the National Institute on Drug Abuse; *Mother Jones* magazine; the United States Information Agency; the American Friends Service Committee; the Consortium on Peace Research, Education, and Development; the gay-themed *Oasis Magazine*; the Stop AIDS Project; and Campaign for Our Children, a nonprofit organization working to prevent teen pregnancy. SmartFilter also blocked sites containing educational information on sexually transmitted diseases, safer sex, and teen pregnancy.

Michael Sims *et al.*, *Censored Internet Access in Utah Public Schools and Libraries* (Censorware Project, Mar. 1999)

The Censorware Project secured Internet log files from Sept. 10-Oct. 10, 1998, of the Utah Education Network, or UEN, a state agency responsible for providing telecommunications services to all the state's public schools and many of its libraries. UEN's Internet access was filtered by SmartFilter. Censorware deemed about 350 Web pages needlessly blocked under one or more of the five categories chosen by UEN: "criminal skills," "drugs," "gambling," "hate speech" and "sex."

Secure Computing claimed that "sites are not added to the Control List without first being viewed and approved by our staff," yet Censorware found that the home page of the Instructional Systems Program at Florida State University was blocked under the "gambling" category, presumably because the word "wager" appears in the URL. (Walter Wager, a member of the program faculty, apparently maintained the site). SmartFilter also blocked "Marijuana: Facts for Teens," a brochure published by the National Institute on Drug Abuse. Censorware's findings also strongly suggested that SmartFilter blocked the entire Wiretap server under the category of "criminal skills" – on account, it seems, of its URL – even though Wiretap consists solely of electronic texts such as presidential inaugural addresses, the Declaration of Independence, Shakespeare's complete plays, *The Jungle Book*, *Moby Dick*, and the Book of Mormon.

SmartFilter blocked "Marijuana: Facts for Teens," a brochure published by the National Institute on Drug Abuse.

Another server entirely blocked, for reasons unclear, was gopher.igc.apc.org, under the "drugs" category; this server of the Institute for Global Communications was home to numerous nonprofit groups, such as the Rainforest Action Network, Human Rights Watch, and Earth First.

In other cases, possibly owing to keyword or URL-based filtering, pages were blocked whose aims were to raise awareness of such issues as hate seech and drugs. Among these

[70] "SmartFilter Control List," www.securecomputing.com/index.cfm?skey=86 (visited 3/3/06).

were Hate Watch, a site monitoring and opposing online hate speech; a scholarly paper titled "'... as if I were the master of the situation': Proverbial Manipulation in Adolf Hitler's *Mein Kampf*," from the archives of *De Proverbio: An Electronic Journal of International Proverb Studies*; the Iowa State Division of Narcotics Enforcement; and a page on the Web site of National Families in Action, a national drug education, prevention, and policy center.

Three months after *Censored Internet Access* was published, Secure Computing issued a press release interpreting the report as a confirmation of SmartFilter's effectiveness. During the period in question, the release stated, "there were over 54 million Web access attempts and of those, according to the report, less than 300 were denied access because the site contacted had been miscategorized. This represents stunning accuracy rate of 99.9994 percent."[71] Similarly, David Burt posted a report in which he claimed that only 279 sites were actually included in Censorware's study, after eliminating sites listed more than once, and that of these, only 64 actually constituted inappropriate blocks. Burt, however, often grouped as one erroneous block what actually amounted to the blocking of multiple distinct pages on a single server.[72]

Jamie McCarthy, "Lies, Damn Lies, and Statistics" (Censorware Project, June 23, 1999)

This was the Censorware Project's response to Secure Computing's and David Burt's claims that its study, *Censored Internet Access*, demonstrated the accuracy of SmartFilter. Author Jamie McCarthy stated that the actual overblocking rate was about 5% because, "for every 22 times SmartFilter 'correctly' blocked someone from accessing a Web page, there was one 'wrongly' blocked access." He also noted that Censorware's investigation did not include sites on SmartFilter's block list that were overridden by the UEN – such as mormon.com, which accounted for 6,434 of the total 122,700 blocked page requests. "Counting these accesses," he wrote, "would raise the error rate from 1 in 22 to 1 in 19." In addition, the approximately 300 blocked sites actually represented 5,601 individual wrongful blocks.

Regarding Burt's analyses of the sites deemed needlessly blocked, Censorware conceded that he was, in a few cases, correct (the sites in question being pornographic after all); yet Secure Computing actually removed them from the SmartFilter database after the first report appeared – and added the Censorware Project's site, in all 27 blocking categories.

Seth Finkelstein, "SmartFilter's Greatest Evils" (Nov. 16, 2000)

Finkelstein found that SmartFilter blocked a number of privacy and anonymous surfing sites, many of which allow users to circumvent filtering software, in every category except "non-essential." He named 19 such services, including www.anonymizer.com; www.freedom.net; www.private-server.com; and www.silentsurf.com. SmartFilter also blocked, under every available classification but "non-essential," many sites providing translations of foreign language Web pages, for instance www.babelfish.org, www.onlinetrans.com, www.voycabulary.com, and www.worldlingo.com. While such sites did not fall within SmartFilter's published blocking criteria at the time, they would very shortly thereafter, with the introduction of SmartFilter 3.0.

Seth Finkelstein, "SmartFilter – I've Got a Little List" (Dec. 7, 2000)

Finkelstein conducted a series of tests with SmartFilter enabled to block only "extreme/obscene" material. Among the blocked sites were one for gay and lesbian Mormons; oth-

[71] Secure Computing press release, "Censorware Project Unequivocally Confirms Accuracy of SmartFilter in State of Utah Education Network" (June 18, 1999).

[72] David Burt, "Study of Utah School Filtering Finds 'About 1 in a Million' Web Sites Wrongly Blocked" (Filtering Facts, Apr. 4, 1999).

ers relating to extreme sports such as desert off-roading, rock climbing, and motorcycle racing; popular music sites devoted to such recording artists as Primus, Tupac Shakur, and Marilyn Manson; the comic book series *Savage Dragon*; illustrator H.R. Giger's home page; Gibb Computer Services, which advertises the "GCS Extreme Series – high performance custom computer systems"; and the official Web site of *The Jerry Springer Show*.

Finkelstein also listed 64 newsgroups blocked by SmartFilter. Among those barred under the "criminal skills" category were the *Telecommunications Digest* and newsgroups maintained by the Computer Professionals for Social Responsibility and the Electronic Frontier Foundation. Newsgroups blocked on the grounds that they contained "cult/occult" material included one for "studying antiquities of the world"; one on Mesoamerican archaeology; 18 pertaining to genealogy; one on the Baha'i religion; a Bible-study group; and 12 others relating to religion, including news:soc.religion.hindu and news:talk.religion.buddhism.

Miscellaneous reports

- Soon after SmartFilter 3.0's introduction, it was cited by Peacefire's "BabelFish Blocked by Censorware" (Feb. 27, 2001) for filtering out AltaVista's foreign language translation service.

SurfWatch

SurfWatch was one of the first filters. Owned by SurfControl (which also now owns Cyber Patrol), as of 2001 it blocked material in five "core" categories: "sexually explicit," "drugs/alcohol," "gambling," "violence," and "hate speech." According to its Web site,

> Before adding any site to our database, each site "candidate" is reviewed by a SurfWatch Content Specialist. Deciphering the gray areas is not something that we trust to technology; it requires thought and sometimes discussion. … We use technology to help find site candidates, but rely on thoughtful analysis for the final decision.[73]

Yet apart from the physical impossibility of personally reviewing every potentially objectionable site, reports of SurfWatch's inaccuracies clearly indicated keyword blocking without human review. SurfControl no longer claims that human beings review every blocked page. Instead, in its 2006 materials the company says that "to give you maximum protection from the threats of harmful and inappropriate Internet content, SurfControl Web Filter incorporates: quality content understanding, Adaptive Reasoning Technology, [and] flexible deployment options," and includes "the industry's largest and most accurate content database with millions of URLs and over a billion Web pages."[74]

Christopher Kryzan, "SurfWatch Censorship Against Lesbigay WWW Pages" (email release, June 14, 1995)

As early as 1995, SurfWatch was criticized for inaccurate and politically loaded blocking. In an email release, Web activist Christopher Kryzan wrote that the recently introduced software blocked 10 of the 30-40 "queer-related sites" he tested, including the International Association of Gay Square Dance Clubs, the Society for Human Sexuality, the University of California at Berkeley's LGB Association, Queer Web, and the Maine Gay Network.

Karen Schneider, *A Practical Guide to Internet Filters* (1997)

TIFAP found SurfWatch blocked nonpornographic sites relating to sexuality (testers

[73] SurfWatch promotional material, www.surfcontrol.com/support/surfwatch/filtering_facts/how_we_filter.html. This Web page no longer exists; in addition to Cyber Patrol, the SurfControl company now offers a product that combines censorship-style filtering with protection against viruses, spyware, and other dangers; see "SurfControl Web Filter," www.surfcontrol.com/Default.aspx?id=375&mnuid=1.1 (visited 3/104/06).

[74] "SurfControl Web Filter," www.surfcontrol.com/general/guides/Web/SWF_Datasheet.pdf (visited 3/14/05).

could not disable SurfWatch's keyword-blocking feature). Though searches for "breast cancer" and "chicken breasts" were allowed, searches for "penis" and "vaginal" were not. Schneider also noted that the filter blocked www.utopia-asia.com/safe.htm, a page of information on safe sex; and www.curbcut.com/Sex.html, "an excellent guide," she wrote, to "sexual activity for the disabled."

Ann Grimes *et al.,* "Digits: Expletive Deleted," *Wall Street Journal* (May 6, 1999)

This column reported that SurfWatch blocked two newly registered domains –www.plugandpray.com and www.minow.com – even though they contained as yet no content, apparently because, "in a setup called 'virtual hosting,'" they shared IP addresses with pornography sites. SurfWatch marketing director Theresa Marcroft "conceded that the company's software tends to block even innocuous virtually hosted sites if they are added to an Internet address that has been previously blocked," although she noted that the company responds quickly to unblock clean sites "once it knows about them." To the Censorware Project's Jim Tyre, this contradicted the company's claim of "thoughtful analysis"; in a response to the *Journal* article, he said Marcroft's revelation affirmed "that claims made by the censorware vendors (most, if not all, not just SurfWatch) that all sites are human-reviewed before being banned are outright lies."[75]

Christopher Hunter, *Filtering the Future* (July 1999)

Hunter reported that SurfWatch blocked 44% of sites he deemed objectionable (16 out of 36), and 7% of nonobjectionable ones (12 out of 164). The nonobjectionable sites included Free Speech Internet Television; *RiotGrrl*; All Sports Casino; Atlantis Gaming site; Budweiser beer, Absolut Vodka; the R.J. Reynolds Tobacco Company; the Adelaide Institute, which is devoted to revisionist history; and the home page of Holocaust revisionist Arthur Butz. While some of these pages may have contained no objectionable material according to the RSAC ratings, they did fall within SurfWatch's published definitions of "gambling," "drugs/alcohol," or "hate speech." But the product then blocked underinclusively in regard to other gambling, drug, alcohol, and hate-related sites, and thus the overall degree of error remained basically the same.

Center for Media Education, *Youth Access to Alcohol and Tobacco Web Marketing* (Oct. 1999)

The CME deemed SurfWatch the most effective of the products it evaluated in preventing access to alcohol and tobacco promotion (it blocked 70% of the promotional-site test sample) though testers could still access a number of sites, including liquorbywire.com; ciderjack.com; and lylessmokeshop.com. SurfWatch also blocked, on average, 46% of promotional sites generated by Yahoo, Go/InfoSeek, and Excite searches, and prohibited one search, for the term "drinking games," altogether. The filter did not block any of the CME's chosen educational or public health sites.

Bennett Haselton, "SurfWatch Error Rates for First 1,000 .com Domains" (Peacefire, Aug. 2, 2000)

Haselton procured an alphabetical list of current dot-com domains from Network Solutions, which maintains a list of every dot-com domain in existence, and eliminated the sites that began with dashes rather than letters. (As "a disproportionate number of these were pornographic sites that chose their domain names solely in order to show up at the top of an alphabetical listing," their inclusion would have rendered the sample insufficiently representative of the domains in question.) From the remaining sites, Peacefire

[75] Jim Tyre, "Sex, Lies, and Censorware" (Censorware Project, May 14, 1999).

culled the first 1,000 active domains, and attempted to access them against a version of SurfWatch configured to filter only "sexually explicit" content.

SurfWatch blocked 147 of the 1,000 domains. After eliminating 96 that were "under construction," Haselton found that 42 of the remaining 51 were nonpornographic, for an "error rate" of 82%. While Haselton wrote that this figure might not be precise given the limited number of domains he examined (the actual error rate potentially being anything from 65-95%), "the test does establish that the likelihood of SurfWatch having an error rate of, say, less than 60% across all domains, is virtually zero." As with other filters tested, Haselton remarked, "we should expect the error rate to be even higher for .org sites that are blocked." And considering the sites that were blocked – such as a-1janitorial.com; a-1sierrastorage com; and a-advantageauto.com – he found highly questionable SurfWatch's claim of "thoughtful analysis."

Bennett Haselton, "Amnesty Intercepted: Global Human Rights Groups Blocked by Web Censoring Software" (Peacefire, Dec. 12, 2000)

SurfWatch blocked a number of human rights organizations under the "sexually explicit" category: Algeria Watch; Human Rights for Workers; the Mumia Solidaritäts Index; the Sisterhood Is Global Institute; the International Coptic Congress; Liberte Aref, which tracks human rights abuses in Djibouti; the Commissioner of the Council of the Baltic Sea States; Green Brick Road, a compilation of resources on global environmental education; and the New York University chapter of Amnesty International. SurfWatch also blocked www.lawstudents.org, an "online legal studies information center."

In its "drugs/alcohol" category, SurfWatch blocked (among other sites) the Strategic Pastoral Action Network; Charter 97, which documents human rights violations in Belarus; and the Kosova Committee in Denmark, whose mission is to advance the human welfare of the Kosova population and support its demands for self-determination. Among the sites blocked for "violence/hate speech" were Parish Without Borders and Dalitstan, an organization working on behalf of the oppressed *Dalits*, or black untouchables, in India.

Peacefire, "SurfWatch Examined" (2000)

SurfWatch blocked as "sexually explicit" various public health and sex education sites, including Health-Net's "Facts about Sexual Assault"; "What You Should Know about Sex & Alcohol," from the Department of Student Health Services at the University of Queensland; "A World of Risk," a study of the state of sex education in schools; and various informational pages on sexually transmitted diseases hosted by Allegheny University Hospitals, the Anchorage Community Health Services Division, Washington University, and the Society for the Advancement of Women's Health Research.

Miscellaneous reports

- A Feb. 19, 1996 *Netsurfer Digest* item ("White House Accidentally Blocked by SurfWatch") revealed that SurfWatch blocked a page on the official White House site (www.whitehouse.gov/WH/kids/html/couples.html), because "couples.html" appeared in the URL. The couples in question were the Clintons and Gores.
- According to an email release from Professor Mary Chelton to the American Library Association Office for Intellectual Freedom list (Mar. 5, 1997), SurfWatch blocked the Web site of the University of Kansas's Archie R. Dykes Medical Library upon detecting the word "dykes."
- On Mar. 11, 1999, Matt Richtel of the *New York Times* reported that SurfWatch

had blocked "Filtering Facts," a filter-promoting site maintained by David Burt.

- According to David Burt's July 14, 1998 expert witness report in the *Mainstream Loudoun* case, SurfWatch prohibited access to 27, or 54%, of sites he considered non-obscene, including Dr. Ruth's official site, the Society for Human Sexuality, Williams College's page on "Enjoying Safer Sex," and five sites dedicated to fine art nude photography.
- The Digital Freedom Network ("Winners of the Foil the Filter Contest," Sept. 28, 2000) reported that SurfWatch blocked House Majority Leader Richard "Dick" Armey's official Web site upon detecting the word "dick."

We-Blocker

We-Blocker is a free filtering service that, as of 2005, blocked sites falling into any of seven categories: "pornography," "violence," "drugs and alcohol," "gambling," "hate speech," "adult subjects," and "weaponry." It found potentially objectionable sites through recommendations from users. Then, "a We-Blocker agent reviews the site – if it is CLEARLY objectionable, it is automatically entered into the database. ... If the site submitted is not clearly objectionable, it is passed to the We-Blocker site review committee who will make the final decision."[76]

Gay & Lesbian Alliance Against Defamation press release, "We-Blocker.com: Censoring Gay Sites was 'Simply a Mistake'" (Aug. 5, 1999)

GLAAD reported that We-Blocker barred the sites of various gay community organizations, including the New York Lesbian and Gay Center and the online news service GayBC.com. After notification, the company unblocked the sites and explained that they had been accidentally added to the software's block list after being "flagged" for the keyword "sex" – and hence the terms "homosexual," "bisexual," and "sexual orientation" – but not reviewed by a We-Blocker employee. "While admirable in its desire to rectify its mistake," the press release stated, "We-Blocker illustrates how imperfect Internet filtering software can be."

WebSENSE

WebSENSE originally operated with 30 blocking categories, including "shopping," "sports," and "tasteless," which could be enabled according to each administrator's needs. The categories were revised with the December 2000 release of WebSENSE Enterprise 4.0, which extended the number to 53 and supplied greater specificity in some of the definitions. "Alcohol/ tobacco," "gay/lesbian lifestyles," and "personals/dating" categories were brought together, along with the new classifications "restaurants and dining" and "hobbies," under an umbrella category, "society and lifestyle." "Hacking" was incorporated into the larger "information technology" category, which also encompassed the previously unaccounted-for "proxy avoidance systems," "search engines & portals," "Web hosting," and "URL translation sites." The "activist" and "politics" categories were combined, as were "cults" and "religion," while "alternative journals" was absorbed into a "news & media" category. Separate subcategories were created for "sex education" and "lingerie & swimsuit."

By July 2005, the WebSENSE database contained more than 10 million sites, organized into over 90 categories. These consist of 31 "baseline categories," such as "adult material," which are then subdivided into such sub-categories as "adult content," "lingerie & swimsuit," "nudity," "sex," and "sex

[76] "We-Blocker Database Criteria," www.we-blocker.com/Webmstr/wm_dbq.shtml (visited 7/21/05). In 2006, this page was no longer available; instead, the URL switched to a page that advised: "We-Blocker is currently undergoing some major programming changes that will greatly enhance the overall speed of the program and improve user-friendliness." "We-blocker.com," weblocker.fameleads.com (visited 3/11/06).

education." Other baseline categories include "advocacy groups," "drugs," "militancy & extremist," "religion," and "tasteless."[77]

In 2002, WebSENSE tried an unusual marketing technique: it began publishing daily lists of pornographic sites that, it said, were not blocked by two of its competitors, SurfControl and SmartFilter. Anybody could access these lists, including students at schools using SmartFilter or SurfControl, simply by clicking a button on the WebSENSE site agreeing that they were over 18. In an attempt to demonstrate the supposed superiority of WebSENSE, the company had thus publicized a set of pornographic sites for easy reference. After five months, WebSENSE ended this experiment. Peacefire reported: "They remain the only blocking software company that has ever tried this technique."[78]

Karen Schneider, *A Practical Guide to Internet Filters* (1997)

Schneider's Internet Filter Assessment Project found that WebSENSE blocked a page discussing pornographic videos but not containing any pornographic material, as well as the entire www.Webcom.com host – because one site that it housed had sexually explicit content.

Censorware Project, *Protecting Judges Against Liza Minnelli: The WebSENSE Censorware at Work* (June 21, 1998)

The Censorware Project examined WebSENSE after learning it had been installed on the computers in three federal appeals courts, and in some Florida and Indiana public libraries. The title of the report was inspired by the authors' discovery that a Liza Minnelli fan page was blocked by WebSENSE as "adult entertainment." Other "grossly inappropriate" blocks, according to Censorware, included the Jewish Teens page; the Canine Molecular Genetics Project at Michigan State University; a number of Japanese-language sports sites (presumably, according to the report, because the software interpreted a particular fragment of transliterated Japanese as an English-language word on its block list); the Sterling Funding Corporation, a California mortgage loan company; the former site of the Safer Sex page, now devoted to AIDS prevention; and a copy of a British Internet service provider's Internet Policy on Censorship.

Michael Swaine, "WebSENSE Blocking Makes No Sense," *WebReview.com* (June 4, 1999)

In June 1999, Webreview.com's Michael Swaine was notified that Swaine's World, his page on technology-related news, had been categorized by WebSENSE as a "travel" site because Swaine had once posted an article about a trade show he attended. Though the block, once brought to WebSENSE's attention, was removed, Swaine writes: "Many Web sites are being inappropriately blocked every day because the blocking schemes are woefully inadequate. WebSENSE explained to me why it had blocked my site, but the explanation was hardly reassuring."

Miscellaneous reports

- The article "Shield Judges from Sex?" in the May 18, 1998, issue of the *National Law Journal* reported that WebSENSE blocked a travel agency site after detecting the word "exotic" – as in "exotic locales."
- In a May 2001 article on various filters' treatment of health information for teens ("Teen Health Sites Praised in Article, Blocked by Censorware"), Peacefire reported that WebSENSE 4.0 blocked www.teengrowth.com as an "entertainment" site.

X-Stop

X-Stop's claim to fame was its "Felony Load," later re-dubbed the "Librarian" edition, which

[77] WebSENSE Baseline URL Categories, www.WebSENSE.com/docs/Datasheets/en/v5.5/WebSENSEURLCats.pdf (visited 7/21/05).

[78] Peacefire, "WebSENSE Examined" (2002).

the manufacturer, Log-On Data Corporation, claimed blocked "only sites qualifying under the *Miller* standard" – referring to the Supreme Court's three-part test in *Miller v. California* for constitutionally unprotected obscenity.[79] This was impossible, because no filter can predict what will be found "patently offensive" and therefore obscene in any particular community. Log-On also asserted that "legitimate art or education sites are not blocked by the library edition, nor are so-called 'soft porn' or 'R'-rated sites."[80]

After a lawsuit was filed challenging the use of X-Stop in Loudoun County, Virginia public libraries, Log-On Data, which had changed its name to 8e6 Technologies, only maintained that "nobody blocks more pornographic sites than X-Stop. We also search out and block sources containing dangerous information like drugs and alcohol, hate crimes and bomb-making instructions."[81] By late 2005, 8e6 Technologies had dropped the X-Stop name but continued to market a variety of Internet filters.

The software relied on an automated "MudCrawler" that located potentially objectionable sites using 44 criteria that were not made public. Borderline cases were allegedly reviewed by "'MudCrawler' technicians." X-Stop also came equipped with a "Foul Word Library," which prohibited users from typing any of the listed terms.

Jonathan Wallace, "The X-Stop Files" (Oct. 5, 1997)

Wallace reported a host of benign sites blocked by a version of X-Stop obtained in July 1997, including The File Room, an interactive archive of censorship cases hosted by the University of Illinois; the *National Journal of Sexual Orientation Law*; Carnegie Mellon University's Banned Books page; the American Association of University Women; the AIDS Quilt site; certain sections of a site critical of America Online (www.aolsucks.org/censor/tos); the home page of the Heritage Foundation; and multiple sites housed on the Institute for Global Communications server, including the Religious Society of Friends and Quality Resources Online.

Peacefire, "X-Stop Examined" (Sept. 1997)

Peacefire reported that 15 URLs blocked by X-Stop's "Felony Load" included the online edition of the *San Jose Mercury News*; a Web site that Peacefire said belonged to the Holy See (eros.co.il); the Y-ME National Breast Cancer Organization; art galleries at Illinois State University; the Winona State University Affirmative Action Office; Community United Against Violence, an organization dedicated to preventing anti-gay violence; the Blind Children's Center; Planned Parenthood; and the entire Angelfire host.

Karen Schneider, *A Practical Guide to Internet Filters* (1997)

Schneider's Internet Filter Assessment Project also found Planned Parenthood blocked, as well as a "safe-sex Web site, several gay advocacy sites, and sites with information that would rate as highly risqué, but not obscene."

Documents in *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*

In 1997, citizens in Loudoun County, Virginia brought a First Amendment challenge to a new policy requiring filters on all library computers. The library board had chosen X-Stop to supply the software, relying on Log-On Data's false claimed that X-Stop blocked only illegal content. In November 1998, a federal court ruled the policy unconstitutional because libraries are "public fora" for the dissemination of "the widest possible diversity of

[79] See the Introduction, page 2.

[80] By 2001, this claim had disappeared from the X-Stop Web site, but it was quoted in the intervenors' complaint in *Mainstream Loudoun v. Board of Trustees of Loudoun County Library*, No. 97-2049-A (E.D. Va. Feb. 5, 1998).

[81] "8e6 Technologies," www.8e6technologies.com (visited 3/13/05).

views and expressions," because the filtering was not "narrowly tailored" to achieve any compelling government interest, and because decisions about what to block were contracted to a private company that did not disclose its standards or operating procedures.[82]

- Plaintiffs' Complaint for Declaratory and Injunctive relief (Dec. 22, 1997)

The original complaint lodged by Mainstream Loudoun reported that X-Stop's "foul word" blocking procedure made it impossible for library patrons to search for the word "bastard" – and thus for such novels as Dorothy Allison's *Bastard Out of Carolina* and John Jakes's *The Bastard*. Also forbidding the term "pussy," X-Stop barred searches for "pussy willows" and "The Owl and the Pussy Cat." On the other hand, the filter allowed searches for "69," "prick," "pecker," "dick," "blow job," "porn," and "nipple."

- "Internet Sites Blocked by X-Stop," Plaintiffs' Exhibit 22 (Oct. 1997)

Plaintiff's Exhibit 22 listed the URLs of 62 sites at one time or another blocked by X-Stop, among them (in addition to many pages also cited by Karen Schneider, the Censorware Project, and others) a page containing information on dachsunds, the Coalition for Positive Sexuality, a page on the Lambda Literary Awards, which recognize "excellence in gay, lesbian, bisexual and transgendered literature," and Lesbian and Gay Rights in Latvia.

- ACLU Memoranda (Jan. 27-Feb. 2, 1998)

An ACLU researcher reported that among the sites blocked by X-Stop at the Sterling branch of the Loudoun County Public Library were www.safesex.org; www.townhall.com, a conservative news site; www.addict.com, which proclaimed itself "addicted to loud noise"; the Queer Resources Directory; and www.killuglytv.com, a teen-oriented site containing health information but also vulgar words. Not blocked were sites promoting

X-Stop barred searches for "pussy willows" and "The Owl and the Pussy Cat."

abstinence as the only safe sex; containing anti-homosexuality material (for instance, a portion of the American Family Association site); and supporting the Communications Decency Act (such as Enough is Enough, Morality in Media, the National Campaign to Combat Internet Pornography, and Oklahomans for Children and Families).

- Plaintiff-Intervenors' Complaint for Declaratory and Injunctive Relief (Feb. 5, 1998)

The intervenors' complaint described the sites of eight plaintiff-intervenors, all blocked by X-Stop, including the *Ethical Spectacle*; *Foundry*, a Web magazine that published the work of painter Sergio Arau; Books for Gay & Lesbian Teens/Youth; the *San Francisco Chronicle*- owned *SF Gate*; the Renaissance Transgender Association, whose mission is "to provide the very best comprehensive education and caring support to transgendered individuals and those close to them"; and Banned Books OnLine, which featured the electronic texts of such famous works as *Candide*, *The Origin of Species*, *Lysistrata*, and *Moll Flanders*. As of October 1997, X-Stop blocked the entire Banned Books site; by February 1998, X-Stop had unblocked most pages on the site, with the exception of Nicholas Saunders's *E for Ecstasy*, which, according to the intervenors' complaint, contained "nothing that could remotely qualify as 'pornographic.'"

- ACLU memoranda (June 17-23, 1998)

ACLU researchers found, in addition to many instances of underblocking, that

[82] *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*, 24 F. Supp .2d 552 (E.D.Va. 1998). It is not clear how much of the court's reasoning survived the Supreme Court's decision in the CIPA case (see the Introduction, pages 2–4).

X-Stop blocked www.gayamerica.com, a collection of links to gay-interest sites; a Dr. Ruth-endorsed site vending sex-education videos; and multiple nonprurient sex-related sites, such as Sexuality Bytes, an "online encyclopedia of sex and sexual health"; the Frequently Asked Questions page of the alt. sex newsgroup, which presented "educational information" on sex, contraception, and sex-related laws, along with textbook-style diagrams and photographs of sex organs; www.heartless-bitches.com, a "grrrls" site with some "harsh language" but no images or "really pornographic" material; and a Geocities-hosted site that contained information on and images of amateur women's wrestling – none of which were pornographic or sexually oriented. Subsequent memoranda reported that X-Stop blocked a page containing information on genital warts; a page discussing, in the researcher's words, "sodomy from a philosophical/postmodernist perspective"; and a site about enemas.

- Report of Plaintiffs' Expert Witness Karen Schneider (June 18, 1998)

Schneider tested X-Stop, using the same methodology she applied in *A Practical Guide to Internet Filters*, with two copies of the program, one purchased in anticipation of her testimony, the other furnished by Log-On Data Corporation. She reported that the filter blocked the page for "Safe Sex – The Manual," which had received an "Education Through Humor" prize at the World Festival of Animated Films; another safe sex education page; a number of sites pertaining to homosexuality, including one that sold gay-themed jewelry; Rainbow Mall, an index to gay-interest sites; and *Arrow Magazine*, an online journal geared for "homosexual men in committed relationships" – on which, according to its self-imposed RSAC rating, neither nudity, sex, nor violence appear.

Schneider also cited some pages allowed by X-Stop: a site containing images of "naked women urinating, in some cases on other people"; Absolute Anal Porn; and two sites featuring images of sexual acts. She concluded that "X-Stop blocks access to a wide variety of Web sites that contain valuable, protected speech, yet fails to block many arguably 'pornographic' Web sites."

- Report of Defendants' Expert Witness David Burt (July 14, 1998)

Burt selected 100 Web sites, 50 of which were "likely to be obscene" and 50 of which were provocative but "clearly did not meet one of the 'obscene' categories."[83] This second 50-site sample comprised 10 soft-core sites, 10 devoted to fine art nude photography, 10 that provided safe sex information, 10 devoted to nude photographs of celebrities (deemed unobjectionable because "this type of pornography almost always consists of simple nudity and partial nudity"), and 10 nonpornographic sites relating to sexuality, such as www.drruth.com and the Coalition for Positive Sexuality. X-Stop blocked 43 of his 50 "likely obscene" sites, or 86%. It left unblocked 70% of the soft-core sites; all but one (or 90%) of the nude celebrity sites (barring only the British Babes Photo Gallery); and all of the art nude, safe sex, and sexuality information sites. Burt determined that, on average, X-Stop allowed access to 92% of his unobjectionable sites. He concluded: "X-Stop is likely the least restrictive filter for blocking obscenity, while [it] is reasonably effective at blocking what are clearly hard-core sites."

- Report of Plaintiffs' Expert Witness Michael Welles (Sept. 1, 1998)

System engineer Michael Welles testified that even with X-Stop installed on his computer, he had easily accessed pornography, and

[83] Burt defined a "likely obscene" site as one featuring any of the following: "1) Photographs showing vaginal, anal, or oral penetration clearly visible; 2) Photographs of bestiality with penetration clearly visible; 3) Photographs of one person defecating or urinating onto another person's face." His categories did not track the legal definition of obscenity; see the Introduction, page 2.

asserted that "one needs a human judge, and a human judge or team of human judges cannot work quickly enough to process the amount of material that is out [on the Web]." Welles concluded that "it is not possible to find a technological method by which a person seeking to establish a blocking system could reliably block sites that must be identified by their subject matter without blocking sites that contain a different subject matter."

- Loren Kropat, Second Declaration (Sept. 2, 1998)

Loudoun County library patron Loren Kropat testified about sites she found blocked using a public Internet terminal on which X-Stop was installed at the Purcellville, Virginia library. Among them were a Washington DC, gay-interest event information site; a profile of Edinburgh; the home page of the Let's Have an Affair Catering company; and www.venusx.com, the Web site of Eyeland Opticians.

Censorware Project, *The X-Stop Files: Déjà Voodoo* (1999; updated 2000)

In 1999, a year after a federal district court ruled the filtering policies of Loudoun County unconstitutional, the Censorware Project published this follow-up to Jonathan Wallace's "The X-Stop Files." It found that Log On Data had removed many of the bad blocks that were identified in the lawsuit, but at the same time introduced more blocks of innocent sites, so that "a year later, the product is no better than it was."

Among the new blocks were Godiva Chocolatier and www.fascinations.com, a dealer in toys relating to physics – in both cases, most likely because "long ago and far away, their domain names belonged to porn sites." X-Stop blocked the home page of *Redbook* magazine, probably because its "meta" description includes the word "sex." On account of supposed explicit sexual content, the filter also barred the academic sites "Sex Culture in Ancient China," which provided a scholarly history of sexology, and Wicked Pleasures, the site for a book on African American sexuality.

Other blocked health and sex-related sites included the Medical Consumer's Advocate; an informational site on massage therapy; a site on alternative medicine; a site on aphrodisiacs, which stated, on its front page, that it did "NOT contain sexually explicit material" (Censorware's emphasis); Great-Sex.com, which sold books and videotapes promoting "clinical and educational sexual wisdom" and contained no nudity; C-Toons, a Web comic serial – intended "to reinforce 'safe sex' attitudes through humor" – whose protagonist was a condom; and Darkwhisper, a site dedicated to "exploring the magic and mystery of sadomasochism" and carrying an adult warning but, according to Censorware, containing "serious text only, not unlike what one can find in many libraries" and hence "a good illustration of the lack of any meaningful human review" by X-Stop.

Still other blocked pages included Home Sweet Loan, a mortgage firm whose URL (runawayteens.com), the report suggested, led to the problematic block; the Thought Shop, a site that at the time of Censorware's investigation contained a commentary opposing the Child Online Protection Act; a Web graphics page called Digital Xtreme!; sites for the recording artists Bombay June and Marilyn Manson; a site posting weather forecasts for the Ardennes region of Belgium; and a page in tribute to Gillian Anderson, which contained no nude images.

X-Stop also blocked every site hosted by the free Web page provider Xoom—a total, at the time of *Déjà Voodoo*'s publication, of 4.5 million distinct sites. Also blocked was the so-called "family-friendly" ISP Execulink, which rated its sites by the RSAC system, offered Bess filtering at the server level, and designated the Focus on the Family Web site a "favorite" link.

Center for Media Education, "Youth Access to Alcohol and Tobacco Web Marketing" (Oct. 1999)

The CME deemed X-Stop "the least effective filter at blocking promotional alcohol and tobacco content," for it did not block any of the selected alcohol- and tobacco-related promotional sites, and blocked just 4% of sites generated by searches for promotional terms—this despite its claim to "block sources containing dangerous information like drugs and alcohol."

Peacefire, "Analysis of First 50 URLs Blocked by X-Stop in the .edu Domain" (Jan. 2000)

Peacefire investigated the first 50 .edu domains on X-Stop's block list as of Jan. 17, 2000. Twenty-four of these, or 48%, were ruled "obvious errors," including a number of innocuous student home pages, a site for a contest in which the grand prize was a boat—possibly X-Stop's MudCrawler was confused, Peacefire wrote, "by the phrase on the rules saying you had to be '18 years or older' to enter the drawing" – and the Paper and Book Intensive, a summer program on the art of the book, papermaking, and conservation, offered by the University of Alabama's School of Library Information Studies. Ten additional URLs, 20% of the overall sample, were found to contain no pornography, but did feature some artistic nudity or harsh language, and were thereby judged "marginal errors."

II. Research During and After 2001

Introduction: The Resnick Critique

Tests of filters' effectiveness between 2001-06 have tended to be more statistical and less anecdotal than many of the earlier studies. This may reflect the fact that filters are now entrenched in many institutions, including schools and libraries. The focus of the more recent studies has therefore shifted from investigating whether filters should be used at all to accepting their existence and investigating which ones perform best. Analysis of performance, of course, depends on underlying, and often subjective, judgments about whether particular Web pages are appropriately blocked.

Methodologies and results have varied in this new world of filtering studies. The lack of consistent standards inspired Paul Resnick and his colleagues to write an article pointing out some of the pitfalls, and making recommendations for good research techniques.[84] It is useful to summarize this article before going on to describe the studies done during and after 2001.

Resnick *et al.* outline four aspects of test design: collecting the list of Web sites that will be used to test the filters, classifying the content of the collected sites, configuring and running the filters, and computing rates of over- and underblocking.

First, they say that in order to avoid bias during the collection of sites for testing, researchers cannot simply pick the sites that they find interesting or relevant, as the authors of a number of studies have done. Instead, testers must use an objective, repeatable process such as collecting all of the sites that a target group of users actually visits, or sampling a well-defined category of sites such as the health listings from particular portals.

Next, they argue that the set of sites used must be large enough to produce statistically valid results and, if the testers intend to evaluate the filters' performance on particular categories of content, that there are enough sites in each category. Thus, they fault several studies that had large test sets overall, but too few sites in each of their many content categories to test the filters' performance in each category.

Resnick *et al.* point out the pitfalls of evaluating whether Web sites are in fact incorrectly blocked. "In order to test whether filtering software implements the CIPA standard, or the legal definition of obscenity," they say, "sites would have to be classified according to those criteria." They add that "if the goal were simply to test whether filtering software correctly implements the vendor's advertised classification criteria, the sites would be independently classified according to those criteria."[85]

The authors also identify two distinct measures for overblocking and underblocking. Each measure is independent and provides different information. Often, researchers use the terms "overblocking" and "underblocking" without specifying which measure they are referring to.

The first measure of overblocking, which Resnick *et al.*, call the "OK-sites overblock rate," is the percentage of acceptable sites that a filter wrongly blocks. The denominator in this fraction is the total number of acceptable sites. This measure gives an indication of how

[84] Paul Resnick, Derek Hansen, & Caroline Richardson. "Calculating Error Rates for Filtering Software," 47:9 *Communications of the ACM*: 67-71 (Sept. 2004).

[85] Resnick *et al.*, 69.

much acceptable, useful, and valuable information a filter blocks.

The second measure, the "blocked-sites overblock rate," is the percentage of blocked sites that should not be blocked. The denominator here is the total number of blocked sites. The measure tells us how common overblocks are relative to correct blocks, but doesn't shed light how a filter affects access to information overall.

To demonstrate the difference, they say, suppose that filter A blocks 99 "OK" sites and 99 "bad" sites, while only leaving one "OK" site unblocked, while filter B blocks only one "OK" site and one "bad" site, leaving 99 "OK" sites unblocked. Both filters have a "blocked-sites over-block rate" of 50%, but filter A's "OK-sites overblock rate" is 99%, while filter B's is 1%. Although both filters have the same ratio of overblocks to correct blocks, filter A has a much greater impact on the availability of information.[86]

Resnick *et al.* also show how the "blocked-sites overblock rate" can be manipulated simply by changing the number of acceptable sites that are in the test set. Because the blocked-sites overblock rate is easily manipulable and can be deceptive, Resnick *et al.* say, the more relevant measure from the vantage point of free expression is the OK-sites overblock rate.

In fact, though, all of the statistical measures are manipulable, depending on the Web sites that researchers choose for their study. As the district court in the CIPA case observed, all statistical attempts to calculate over- and underblocking rates suffer from the difficulty of identifying a truly random sample of Internet sites, or—the relevant inquiry for purposes of that case—a sample that truly approximates "the universe of Web pages" that library patrons are likely to visit.[87]

Resnick *et al.*'s clarifications are valuable, but calculating error rates, regardless of how carefully it is done, will always be misleading for a medium as vast as the Internet. It is rarely possible to know in advance whether a Web site would violate CIPA, and it is even more difficult to agree on whether a site meets such broad filtering categories as "tasteless," "intolerance," or "alternative lifestyle."

In short, using statistics to gauge how well filters work can be deceptive. Even a 1% error rate, given the size of the Internet, can mean millions of wrongly blocked sites. The statistical approach also assumes that Web sites are fungible. If only 1% of "health education" sites are wrongly blocked, for example, the assumption is that those searching for health information can find it on another site that is not blocked. But different Web sites have different authors, viewpoints, and content (not all of it, of course, necessarily accurate). From the perspective of free expression, even one wrongly blocked site constitutes censorship and is cause for concern. It may be the very site with the information you need. Certainly, it is not much consolation to the publisher of the site that a Web searcher can access another site on the same general topic.

With this introduction to the pitfalls of filter testing in mind, we turn to the studies conducted during and after 2001 that sought to test over- and underblocking. Our summaries are presented chronologically.

Report for the Australian Broadcasting Authority

Paul Greenfield, Peter Rickwood, & Huu Cuong Tran, *Effectiveness of Internet Filtering Software Products* (CSIRO Mathematical and Information Sciences, Sept. 2001)

Australian government regulations require

[86] Resnick *et al.* similarly identify two measures of underblocking: the "bad-sites underblock rate" (the percentage of "offensive" sites that the filter fails to block), and the "unblocked-sites underblock rate" (the percentage of unblocked sites that should have been blocked under the manufacturer's criteria). Like the two measures of overblocking, these numbers give very different information about filters' performance.

[87] *American Library Ass'n v. U.S.*, 201 F. Supp. 2d at 437-38.

most of the country's Internet service providers to offer their customers an optional filter from a list of approved products compiled by the Internet Industry Association (IIA). This study, commissioned by the Australian Broadcasting Authority and the nonprofit organization NetAlert, evaluated 14 of the 24 filtering products that were on the IIA list as of February 2001.[88]

The study evaluated the filters based on their ability to block content the researchers deemed objectionable without blocking content they deemed innocuous, and on other criteria such as reliability, cost, and ease of use. It also tested whether the product could be deactivated by a filter-disabling tool created by Peacefire. The filters were tested against 895 Web sites taken from 28 categories developed by the authors, containing at least 20 sites each.[89] These categories included both those likely to contain sites that the testers thought objectionable (*e.g.*, "pornography/erotica," "racist/supremacist/Nazi/hate," and "bomb-making/terrorism"), and those that they deemed likely to include unobjectionable content such as "sex education." "gay rights/politics," "drug education," "art/photography," and "filtering information." The 28 categories also included such other subjects as "swimsuit models," "glamour/lingerie models," "sex laws/issues," "atheism/anti-church," "anarchy/revolutionary," and "politics."

The report did not provide a list of the Web sites that were tested and did not specify how those sites were collected. It presented results in the form of rough percentages instead of exact figures. It did not report the number of sites erroneously blocked by any of the filters. Nor did it state the criteria that were used to categorize the sites or to decide whether a given site should be classified as objectionable.

Most problematic, perhaps, the authors did not make clear whether they thought that all, some, or none of the sites that they placed in categories like "art/photography," "nudism," or "atheism/anti-church" should be blocked. They did not explicitly say whether they found these sites objectionable or not. And since they generally tested the filters at their maximum settings, which were designed to block categories such as nudity or sex education, the authors could hardly rate these filters inaccurate simply because they blocked large amounts of worthwhile material in these categories.

All of the products tested used some combination of three techniques: blocking all of the sites on the Internet except those found on a whitelist of allowed sites; blocking only those sites found on a blacklist while allowing the rest; and blocking all sites that contain words, phrases, or in the case of Eyeguard, images that are deemed objectionable. The researchers found that the two products that used whitelists—the "Too C.O.O.L." children's Web browser and the "Kids Only" setting of America Online (AOL) Parental Controls—blocked almost all of the sites that they tested in all of the categories.[90]

Of the products that used blacklists and word or phrase-based filtering, N2H2 set to "maximum filtering" was the most effective at blocking sites in the categories that the researchers deemed objectionable—about 95% of the sites in the "pornography/erotica" category, about 75% of those qualifying as

[88] The products tested were: AOL Parental Controls 6.0; Cyber Patrol 5.0; Cyber Sentinel 2.0; CYBERsitter 2001; Eyeguard, version not specified (our research indicates that this product is no longer on the market); Internet Sheriff, version not specified; I-Gear 3.5 (name later changed to Symantec Web Security); N2H2, version not specified; Net Nanny 4.0; Norton Internet Security 3.0, Family Edition; SmartFilter 3.0; Too C.O.O.L. (which seems to have been discontinued), version not specified; and X-Stop 3.04 (now called 8e6 Home).

[89] The text of the report says 27 categories at one point, and 24 at another, but an accompanying table lists 28. Greenfield *et al.*, 23, 25-26, 31.

[90] Two other products, Eyeguard and Cyber Sentinel, "were not automatable using our test tools and had to be tested manually, and as a result were not evaluated against the complete site list." Greenfield *et al.*, 26.

"bomb-making/terrorism," and about 65% of those qualifying as "racist/supremacist/Nazi/hate." But it also blocked many of the sites in potentially unobjectionable categories, including about 60% in "art/photography," about 40% in "sex education," about 30% in "atheism/anti-church," about 20% in "gay rights/politics," and about 15% in "drug education." I-Gear and the "Young Teen" setting of AOL Parental Controls performed similarly—they blocked nearly as many of the sites in the categories deemed objectionable, but also blocked a substantial portion of the sites in potentially unobjectionable categories.

Eyeguard's Image analysis blocked all images that contained colors resembling Caucasian skin tones, including innocuous pictures of faces and desert scenes.

Judged by their ability to block sites the researchers thought objectionable without blocking too many potentially unobjectionable sites, AOL's "Mature Teen" was rated the best performer. It blocked about 90% of the sites in the "pornography/erotica" category, 60% of those in "racist/supremacist/Nazi/hate," and 25% of those in "bomb-making/terrorism," while blocking about 15% in "sex education," 10% in "gay rights/politics," and 5% in "drug education." SmartFilter performed nearly as well, according to the researchers.

The rest of the products were substantially worse. CYBERsitter, Cyber Sentinel, Norton Internet Security, and Internet Sheriff blocked virtually as many potentially unobjectionable sites as N2H2 and I-Gear while blocking fewer sites that the researchers deemed objectionable. Although Cyber Patrol, Net Nanny, and X-Stop blocked relatively few potentially unobjectionable sites, they did not block many of the sites that the researchers thought objectionable either.

Finally, despite the fact that Eyeguard, which uses image analysis to try to identify pornographic images, managed to block about 80% of the sites in the "pornography/erotica" category, it did not block other content that the researchers deemed objectionable, such as "racist/supremacist/Nazi/hate" or "bomb-making/terrorism." Its image analysis also blocked about 65% of the sites in the "art/photography" category. In fact, Eyeguard's image analysis blocked all images larger than a certain size that contained colors resembling Caucasian skin tones, including innocuous pictures of faces and desert scenes. At the same time, it failed to block pornographic images that were black-and-white, were small in size, or had unusual lighting.

Some of the filters had other quirks. Cyber Sentinel's keyword filtering blocked all content in Web browsers, chat programs, and even word processing programs containing words deemed objectionable without regard to their context. Thus, Cyber Sentinel blocked a nudist site containing the phrase: "This site contains no pornography. It contains no pictures of male or female genitals …," because it used the words "pornography" and "genitals."[91] CYBERsitter and Cyber Sentinel both blocked about half the sites tested that discussed Internet filtering products.

The authors acknowledge the difficulty of judging filters based on their capacity to block "objectionable" content. Lists of sites for testing, they say, "reflect the values of the organizations and people who compile them … Cultures differ considerably in their concepts of 'acceptable' content."[92]

[91] Greenfield *et al.*, 46.

[92] *Id.*, 6.

"BESS Won't Go There"

Valerie Byrd, Jessica Felker, & Allison Duncan, "BESS Won't Go There: A Research Report on Filtering Software," 25:1/2 *Current Studies in Librarianship* 7-19 (2001)

Byrd and two fellow South Carolina librarians evaluated five commercial filtering products with an eye toward their suitability for library use.[93] They compiled a list of 200 search terms from medical and slang dictionaries and from their own brainstorming, and then partitioned this list into "bad" and "good" terms. From these lists, they chose 10 "good" and 10 "bad" terms at random,[94] entered each into the Google search engine, and tested the filters against the first 10 hits that each search returned. Each filter was tested against a total of 200 URLs.

To decide whether the sites they collected were "acceptable" or "unacceptable," the researchers combined criteria from the Federal Communications Commission's "indecency" standard, the Child Online Protection Act (COPA), and the America Online Terms of Service. They defined "acceptable" sites as those containing: "mild expletives"; "non-sexual anatomical references"; "photos with limited nudity in a scientific or artistic context"; "discussion of anatomical sexual parts in reference to medical or physical conditions"; "graphic images in reference to news accounts"; and "discussions of drug abuse in health areas." They defined "unacceptable" sites as containing: "actual or simulated sexual act or contact"; "actual or simulated normal or perverted sexual act"; "lewd exhibition of genitals or post-pubescent female breasts"; "blood and gore, gratuitous violence"; and "discussions about or depictions of illegal drug abuse." Their final definition, which they posed as a rhetorical question, was that sites are unacceptable ("obscene") if "they lack literary, artistic, political, or scientific value."[95]

After evaluating the sites they collected, the researchers decided that 94% of the ones they found using the "good" search terms were "acceptable." But 65% of the sites found using the "bad" search terms were also "acceptable" to them, and therefore should not be blocked in public libraries.

A major problem with this article is that Table 2, on which the researchers summarize their findings, is not clear on what it is reporting. The table contains two columns, one for the "good words" and one for the "bad words." The first box in each column gives percentages of "acceptable" and "unacceptable" sites within the 200-site sample. The succeeding boxes give blocking percentages for each filter. These boxes seem to be reporting simply the percent of sites blocked by each filter using "good" and "bad" search terms. But it makes little sense to report such results, because they tell us nothing about how many "acceptable" and "unacceptable" sites were blocked. Reading this ambiguous table as instead reporting the percentages of "acceptable" and "unacceptable" sites blocked using both "good" and "bad" search terms" is more consistent with the text of the report, which describes results in terms of blocking "acceptable" and "unacceptable" sites. But it is not entirely consistent, as the following example suggests.[96]

[93] The five products tested were: Fortres 101; Cyber Patrol; CYBERsitter; the "Mature Teen" setting of America Online Parental Controls; and Bess. The product versions were not specified, and the report did not indicate which configuration of Cyber Patrol, CYBERsitter, and Bess were used. Fortres 101, they reported, is not really a filter; it is simply software that allows users to enter sites they would like blocked. Accordingly, it did not block any of sites tested. (It was included in the study because it was being used in at least one South Carolina school district.)

[94] The "good" terms were: "anonymous sex," "barnyard," "bite," "blossom," breast cancer," "colon cancer," "Dick Cheney," "ovarian cancer," "pictures," and "White House." The "bad" terms were: "babes," "bestiality," "bitch," "boner," "bong," "butt," "cock," "cunt," "fuck," and "porn."

[95] Byrd et al., 12.

[96] In February 2005, Ariel Feldman wrote to Valerie Byrd requesting clarification on several questions of methodology, as well as back-up data. She replied in March that she and the other researchers "have all been looking for the requested information, but unfortunately, we have come up with nothing." Email correspondence between Ariel Feldman and Valerie Byrd, Feb.-Mar. 2005. We received no reply to a follow-up inquiry to Valerie Byrd in March 2006, specifically addressing the ambiguity in Table 2.

The researchers write that Cyber Patrol failed to block "unacceptable" sites 69% of the time. Depending on how one reads Table 2, however, Cyber Patrol either failed to block 69% of the sites found using "bad" search terms, or it failed to block 69% of "unacceptable" sites found using "bad" search terms. It also failed to block 91% of the sites found using "good" search terms, or—following the other possible reading of Table 2—it failed to block 91% of the "unacceptable" sites found using "good" search terms. If we think that Table 2 refers to blocking rates for "acceptable" and "unacceptable" sites, we would have to merge Cyber Patrol's 69% underblocking rate using "bad" search terms with its 91% underblocking rate using "good" search terms, for an average of 80% underblocking. Either way, the text of the article is inconsistent with the table that summarizes the findings. Because of these ambiguities and inconsistencies, the numbers reported in the study are not very meaningful.

The researchers did not specify any of the sites they deemed acceptable or unacceptable, but they did, "just for fun," sit down at a computer and test the filters outside the contours of their formal study. With Bess, they found that they could not access information about the film, "Babes in Toyland," nor could they find out who won Super Bowl XXX. Bess sometimes appeared to replace the sites it deemed unacceptable with other Web sites, but this did not happen consistently. Bess blocked all Web sites that included the word "vaginal," which left out a number of women's education health sites.[97]

Bess, they decided, blocked "too much acceptable information for it to be considered a successful filter." They felt that AOL "Mature Teen" setting "seems to be the most accurate as far as the number of sites blocked compared to the number of unacceptable sites." But then they said: "We believe that for those who prefer to use a filter, the best choice is CYBERsitter. It did not block cancer sites or other acceptable sites."[98]

[97] Byrd *et al.*, 16

Report for the European Commission: Currently Available COTS Filtering Tools

Sylvie Brunessaux *et al.*, *Report on Currently Available COTS Filtering Tools, D2.2, Version 1.0* (MATRA Systèmes & Information, Oct. 1, 2001)

Sylvie Brunessaux and her colleagues evaluated 10 commercial filtering products and collected basic information about 40 more as part of the "NetProtect" initiative, designed to produce a prototype anti-pornography filter that "takes into account European multilingual and multicultural issues."[99] They ranked the filters according to numerical scores based on their ability to block pornographic content from sites in five European languages (English, French, German, Greek, and Spanish), on their rates of overblocking, and on other criteria such as reliability, cost, and ease of use.[100]

The researchers tested the filters against 4,449 URLs in the five different languages, of which 2,794 represented sites they deemed pornographic, and 1,655 sites they deemed "normal."[101] They collected the URLs of the pornography sites both by entering terms like "sex" into search engines, and by following links from personal Web pages, chatrooms, and other sources. For content they deemed normal, they collected both the URLs of sites that they did not expect would confuse

[98] *Id.*, 12, 15. Note that in other studies, CYBERsitter was found highly inaccurate and ideologically biased.

[99] Sylvie Brunessaux *et al.*, 5.

[100] The 10 filters tested were: BizGuard Workstation 2.0 (available from Guardone.com); Cyber Patrol 5.0; CYBERsitter 2001; Cyber Snoop 0.4 (manufactured by Pearl Software); Internet Watcher 2000 (manufactured by Bernard D&G); Net Nanny 4; Norton Internet Security 2001 Family Edition 3.0; Optenet PC; SurfMonkey; and X-Stop (now called "8e6 Home"). Of these, BizGuard and SurfMonkey Web sites can no longer be found. "COTS" stands for "commercial off-the-shelf."

[101] Throughout the report, they use the term "harmful" as equivalent to pornographic.

filters, such as Web portals, news sites, and sites designed for children, and the URLs of sites they thought would confuse filters, such as sex education sites, sites dedicated to gay and lesbian issues, and nonpornographic sites that contained ambiguous words like "kitty," pussy," or "gay."

They tested the 10 filters using a program called CheckProtect since, as they explain, "given the huge number of URLs tested, it was not possible to do the test manually."[102] The results for both under- and overblocking are given in statistical form; no specific Web sites are identified. In fact, the report only once mentions an individual site—when an optional feature of Internet Watcher 2000 redirected traffic from blocked pages to the Web site of the Coca Cola Company.[103]

The researchers configured each filter to what they called its "most secured profile (i.e., the youngest in most cases)."[104] They found that none of the products fared well when tested against their collected sites in five languages. The product that was most effective at blocking pornography, Optenet, only managed to block 79% of these sites, while blocking 25% of the sites considered harmless, including 73% of those pertaining to gay and lesbian issues, 44% of those devoted to sex education, 43% of those containing ambiguous words, and 14% of those designed for children. These numbers support the perception, later articulated by experts during the CIPA trial, that the more effective filters are at blocking pornography (or other disapproved content), the more they are likely to overblock "normal" sites.

Cyber Snoop and SurfMonkey also performed poorly—each blocked only 65% of the sites deemed pornographic while blocking large numbers of innocuous sites. Cyber Snoop blocked 59% of the sites devoted to sex education, 55% of those pertaining to gay and lesbian issues, and 29% of those containing ambiguous words. SurfMonkey blocked 22% of the sites devoted sex education, 20% of those containing ambiguous words, and 13% of those on gay and lesbian issues.

The remaining filters were similarly flawed. None blocked more than 55% of the content deemed pornographic while the worst, Net Nanny, only managed to block 20%. Despite their low effectiveness, BizGuard and Norton Internet Security also significantly overblocked.

On average, the filters blocked only 52% of the sites deemed pornographic in all five languages. This rate rose to 67% when only the English sites were considered, which suggests the difficulty of compiling lists of "bad" keywords in multiple languages. As for overblocking, the average rate for all of the products was 9%. But this is somewhat deceptive because many of the sites considered nonpornographic were relatively uncontroversial and easy to classify, such as Web sites for children, news sites, and search engines. The overblocking rates were much higher for the kinds of sites that typically are problematic for filters—sex education, gay and lesbian issues, and sites containing ambiguous words, which had 19%, 22%, and 13% overblock rates respectively.

On the other hand, given that the filters were tested at their most restrictive settings, it is not surprising that they blocked large numbers of gay and lesbian or sex education sites. Even though nonpornographic, these are precisely the sites that many filters are designed to block. If, as they reported, the researchers were only interested in finding the most accurate filter for blocking pornography while allowing access to educational materials, they should have set the filters at their "adult/sexually explicit" or "pornography" settings, rather than their "most secured profile."

[102] Sylvie Brunessaux *et al.*, 23.

[103] *Id.*, 60.

[104] *Id.*, 23.

The researchers concluded by ranking the filters according to numerical scores, but those scores were based on many factors, of which filtering effectiveness was only one. In fact, the products with the two highest overall scores, CYBERsitter and Internet Watcher 2000, scored poorly on blocking pornography, with rates of 46% and 30% respectively. The researchers expressed surprise that many commercial products had such high rates of error.

This report formed the basis for a later "Final Report" in June 2002, which lists one author, Stéphan Brunessaux. The later document states that it is an "edited version" of the original "restricted final report that was sent to the Commission."[105] In fact, it is a very different, and much shorter, report, which summarizes nine separate documents that were produced during the NetProtect project.

The major difference between the lengthy "restricted" report and the briefer Final Report is that the initial report criticized the performance of all the products tested. The Final Report states that NetProtect has been successful and that a prototype filter using Optenet has now been created.[106] Both reports, however, acknowledge the "problems of current existing filtering solutions: inappropriate blocking/filtering techniques which sometimes block legitimate Web sites and occasionally allow questionable Web sites, inability to filter non-English Web sites and therefore most Web European sites, [and] lack of transparency, disabling the user [of] the right to know why some sites can be accessed and not others."[107]

The Final Report notes that the prototype filter includes image-recognition as well as text-based filtering. It points to the "value of combining [these] different techniques," even while acknowledging that image-based programs "are not able to distinguish between what is just skin and what is nudity and much less what is pornography."[108] In fact, one of the other NetProtect reports found that image-based filters blocked pictures of deer, sheep, dogs, penguins, and other animals. That report is described below.

Report for the European Commission: Filtering Techniques and Approaches

Ana Luisa Rotta, *Report on Filtering Techniques and Approaches, D2.3, Version 1.0* (MATRA Systèmes & Information, Oct. 23, 2001)

Rotta examined five products that use image analysis, four that use text-based filtering, and three that combine the two methods.[109] Originally, she intended to test these tools using the same 4,449 URLs assembled by Sylvie Brunessaux for the *Report on Currently Available COTS Filtering Tools*, discussed above; but this was not possible for technical reasons. In the end, it appears that Rotta did not test some of the products, but instead reproduced information from other sources. For other products, she used different lists of URLs for testing.

Like Brunessaux, Rotta used CheckProtect to run her tests, and evaluated the products based not only on their effectiveness (over- and underblocking), but on such factors as speed, ease of integration with other applications, and facility at blocking in different languages. Focusing on effectiveness, she concluded that three "text-based" products (Optenet, The Bair, and Puresight) failed to block about 40% of pornographic Web

[105] Stéphan Brunessaux, *Report on Currently Available COTS Filtering Tools, D5.1, Version 1.0* (MATRA Systèmes & Information, June 28, 2002), 4. See "NetProtect Results" for links to all of the documents, np1.net-protect.org/en/results.htm (visited 2/28/06).

[106] Stéphan Brunessaux, 5.

[107] *Id.*; Sylvie Brunessaux *et al.*,5.

[108] Stéphan Brunessaux, 9, 17.

[109] The text-only products were Optenet; Contexion Embedded Analysis Toolkit (EATK), manufactured by Rulespace; Puresight; and Sail Labs Classifier. The image-analysis products were Eyeguard; First 4 Internet; LookThatUp Image Filter; EasyGlider; and WIPE Wavelet Image Pornography Elimination. The three hybrid products were The Bair Filtering System, Filterix, and Web Washer EE.

sites; their overblock rates ranged from 6.2-18.12%.[110] Since we do not know what database of URLs was used, these rates of over- and underblocking are not very meaningful.

Rotta gives no test results, but only a product description, for Contexion/Rulespace. For Sail Lab Text Classifier, described as an "automatic text classification" system, Rotta assembled a database of 369 pornographic and 110 nonpornographic URLs, along with about 5,000 Reuters news articles. She reported 97% effectiveness, .3% overblocking overall, but 13% overblocking if measured on a set of "specially collected nonpornographic URLs."[111]

The five image-recognition filters are covered in similarly disjointed fashion. Rotta describes Eyeguard, in language seemingly drawn from its promotional literature, as a technology that "checks the images being displayed for excessive skin tones, thereby protecting the user from pornographic images"; evidently, no testing was done. Similarly, there are no tests reported for EasyGlider. For First 4 Internet, described as an "artificial intelligence" technology that analyzes images to determine if they have "attributes of pornographic nature," Rotta states that a company called TesCom found 95% effectiveness at blocking pornography, but that it gave no indication of the rate of overblocking. Similarly, for WIPE Wavelet, she reports only tests done by others, which found over 96% effectiveness at identifying pornography, but overblocking rates of 9-18%.[112]

Rotta did test LookThatUp, described as "a highly sophisticated system of algorithms based on image techniques," which rates images for pornographic content on a scale of 1-100. She used 100 "harmful images" and 100 "harmless" ones for testing. Of the 100 "harmful" images, the filter failed to analyze 27; of the remaining 73, its pornography-identifying scores for a quarter of them were below 70%—that is, it failed to recognize them as clearly pornographic. Of the "harmless" images, which included animals, clothed people, and nonpornographic nudes, the filter scored almost a quarter of them at above 70%—that is, it identified them as pornography. Among the misidentified images were a woman in a swimsuit waterskiing and a pair of deer in a forest. In a second test of 100 nonpornographic images (landscapes, famous places, animals), LookThatUp did somewhat better, but still gave high "porn scores" to images of sheep, dogs, koalas, and penguins. Overall, the filter identified 24% of "potentially harmless pictures" and 8% of "harmless pictures" as pornographic.

Despite these results, Rotta concluded that LookThatUp can "bring an added-value to an integrated solution as the one we intend to develop in the context of the NetProtect project."[113] The goal seemed to be maximum porn-blocking without regard to how many pictures of animals, landscapes, or other nonpornographic content are also eliminated.

Reports From the CIPA Litigation

A number of empirical studies of filter effectiveness were introduced in evidence during the trial of the lawsuit challenging CIPA. We summarize these reports below.[114] The researchers who conducted these studies were cross-examined in court, but in order to keep this report to a manageable size—and also be-

[110] The Bair is listed as a hybrid in the table of contents, but is designated as a text-based product later in the report. Rotta, 17.

[111] Rotta, 24-25.

[112] *Id.*, 26-36.

[113] *Id.*, 32.

[114] Three of the reports from the CIPA case are not described here. One, by Christopher Hunter, is described in Part I, pages 17–18. We were unable to locate two others, from librarians Michael Ryan (for the plaintiffs) and David Biek (for the government). See note 121 for the district court's description of Ryan's testimony. The court gave Biek's testimony little credence. *American Library Ass'n v. U.S.*, 201 F. Supp. 2d at 441-42.

cause the authors of the other tests and studies we describe were not cross-examined—we won't attempt to summarize the cross-examinations. We do note points where the district court judges commented on the empirical reports.

Geoffrey Nunberg, a scientist at the Xerox Palo Alto Research Center and a professor at Stanford, also served as an expert witness, providing the court with background on the operation and effectiveness of filters. Although Nunberg did not present any test results, it is useful to summarize his report because the three district court judges relied on it extensively in their decision striking down CIPA.[115]

One filter gave high "porn scores" to images of sheep, dogs, and penguins.

Nunberg's report explained first that filter manufacturers locate most of the sites they classify by following the hyperlinks on Web pages accessible through search engines and directories. But since only a minority of Web pages are accessible through search engines and many pages cannot be reached through simple hyperlinks, filter manufacturers actually classify only a small fraction of the Web.[116]

Second, Nunberg said that most filters classify sites automatically, based on their text. This method is flawed because even the most sophisticated text classification systems, including those described as "artificial intelligence," are easily confused and are incapable of taking context into account. Filters that classify based on images are even worse, and are easily fooled by flesh-colored pictures of pigs, pudding, and Barbie dolls.

Next, Nunberg explained that, in an effort to keep up with Web sites' changing names and reduce the number of pages they have to review, filtering manufacturers often block sites by their IP addresses instead of names, and block whole sites after reviewing only a handful of their pages. These shortcuts lead to substantial overblocking because a single IP address can correspond to multiple Web sites, not all of them necessarily "objectionable," and because sites that contain a few "objectionable" pages may contain thousands of "acceptable" ones. He added that filters usually block language translation, anonymizer, and Web caching sites because, as a side effect of their operation, such sites can be used to bypass filters.[117]

Finally, Nunberg said that the use of human reviewers is inherently limited. Despite filter manufacturers' claims to the contrary, it is impossible for all of the sites on filters' block lists to be reviewed individually. Moreover, there are numerous errors even among the sites that are hand-screened because the people hired to review sites are often poorly trained and more concerned with blocking anything that might offend some of their customers than with avoiding overblocking. He also pointed to instances in which screeners have deliberately blocked sites critical of filters.

Nunberg noted, among examples of wrongly blocked sites: an article on "compulsive hair pulling" on a health information site, blocked by N2H2, probably because other articles on the site pertained to sexual health; a bulletin board called "penismightier.com," blocked by N2H2 and SmartFilter, probably because an automatic text filter detected the word "penis" in the site name; and an article on Salon.com criticizing Bess, which Nunberg thought was probably blocked by N2H2 deliberately.

Nunberg pointed out that there is always a tradeoff between efficiency in blocking

[115] A decision reversed by the Supreme Court, but not because of any disagreement with the district court's fact-findings regarding the operation of Internet filters; see the Introduction, pages 3-4.

[116] Expert Report of Geoffrey Nunberg in *American Library Ass'n v. United States.*

[117] See Benjamin Edelman's separate study on this issue, page 64.

presumably offensive sites and overblocking of valuable sites. Because they are such crude tools, filters designed to minimize overblocking will also be less effective at the job they are supposed to do.

Nunberg concluded that it is impossible for filters to get much better. Computerized classifiers lack the knowledge and human experience that are crucial to comprehending the meaning of texts. Computers certainly lack the subjective judgment to understand a legal definition of obscenity that even human beings cannot agree on. Finally, the sheer size of the Internet makes it impossible to replace automatic classification with human screeners. In fact, Nunberg observed that the entire staffs of all the filter manufacturers combined could not review the new sites that are added every day, let alone classify every site on the Web.

Initial Report of Plaintiffs' Expert Benjamin Edelman (Oct. 15, 2001)

Benjamin Edelman, a systems administrator and multimedia specialist at Harvard's Berkman Center for Internet and Society, tested Cyber Patrol, N2H2, SmartFilter, and WebSENSE against a list of nearly 500,000 URLs that he collected.[118]

Edelman collected the URLs, first, by gathering a substantial portion of those listed in the Yahoo! Directory under nonpornographic categories such as "arts," "business and economy," "education," and "government." He expanded this list by locating similar sites using Google's "related" function; and adjusted it based on recommendations from the plaintiffs' attorneys. He then used an automated system to run this list through each of the filters, and recorded which Web pages were blocked. He configured each of the filters to block sites that contained "adult content," "nudity," "sex," and "pornography." He updated the filters' block lists before running them and archived a copy of each blocked site as it appeared when it was tested. This process yielded a list of 6,777 pages blocked by at least one of the four filters. Portions of this list were then given to plaintiffs' experts Joseph Janes and Anne Lipow for analysis.

Edelman's results showed very little agreement among the filters on which content should be blocked. Only 398 Web pages out of 6,777 were blocked by all four of the filters, and the vast majority—5,390—were blocked by only one. N2H2 was the most restrictive, blocking nearly 5,000 pages as compared to the other three filters, which blocked between 1,500 and 2,200. In fact, N2H2 blocked nearly 3,000 sites that were not blocked by any other filter.

Edelman also offered insights gleaned from depositions of filter company representatives that were taken in preparation for the CIPA trial. The representatives admitted that despite studies indicating that effective human screening of the Web would require a staff of thousands, their companies each employed 8-40 screeners, some of whom only worked part-time. The representatives also admitted that their companies almost never reexamine sites they have already classified, and rarely evaluate the accuracy of their employees' ratings. And despite some manufacturers' continuing claims that every site they block has been evaluated by a human screener, an N2H2 official admitted that sites classified as pornography by its automatic classification system are often added to its block list without review. Edelman's own research confirmed this lack of human review: for example, "Red Hot Mama Event Productions" was blocked by SmartFilter and Cyber Patrol, and www.the-strippers.com, a furniture varnish removal

[118] This figure is not mentioned in Edelman's report, but it appears in the district court opinion, 201 F. Supp. 2d at 442. The filters tested were: Cyber Patrol 6.0.1.47; N2H2 Internet Filtering 2.0; SmartFilter 3.0.0.01; and WebSENSE Enterprise 4.3.0. Edelman also gave an overview of the design and operation of Internet filters, mentioning several of the flaws that Geoffrey Nunberg also discussed.

service, was blocked by Cyber Patrol and WebSENSE.

Report of Plaintiffs' Expert Joseph Janes (Oct. 15, 2001)

Joseph Janes, a professor at the University of Washington, was asked to determine how many of the 6,775[119] sites that plaintiffs' expert Benjamin Edelman found to be blocked by four Internet filters contained material that belonged in libraries. Janes and 16 reviewers recruited from the university's Information School, five of whom had extensive experience in building library collections and 11 of whom had less experience, evaluated a randomly selected sample of 699 of the blocked sites.

Janes divided the 699-site sample into groups of about 80 sites each, and ensured that each group was evaluated by two of the less experienced judges. If both of these judges agreed that a site belonged in libraries, the site was considered appropriate. Otherwise, it was submitted to the more experienced judges, who then made a final decision on its appropriateness.

To be considered appropriate, a site had to contain information:

- similar to that already found in libraries;
- that a librarian would want to have, given unlimited space and funds; or
- that a librarian would recommend to a patron who appeared at the reference desk.

The judges were told to consider sites with only erotic content to be inappropriate, and sites that were primarily commercial in nature to be appropriate.

Janes's judges concluded that 474, or 68% of the 699 sites sampled, contained material that belonged in libraries. Extrapolating to the 6,775 total blocked sites, Janes concluded that 65-71% of them were wrongly blocked.

[119] Not 6,777 because of errors in data processing. See *Initial Report of Benjamin Edelman,* 9.

Even taking into account some valid criticisms of Janes's methods, the district court credited his study "as confirming that Edelman's set of 6,775 Web sites contains at least a few thousand URLs that were erroneously blocked by one or more of the four filtering programs" that were tested.[120]

Report of Plaintiffs' Expert Anne Lipow "Web-Blocking Internet Sites: A Summary of Findings" (Oct. 12, 2001)

Anne Lipow, a consultant and former librarian, was asked to determine how many of a sample of 204 sites contained material that a librarian would either want to have, or would be willing to recommend to a patron. The sample was taken from Edelman's list of 6,777 sites blocked by one or more of the filters he tested.[121]

Lipow examined the home page and several other pages on each site; then put them into one of four categories: (A) high quality information that a librarian would want in a library; (B) useful information, but that would not be included in a library collection because of limited usefulness to most patrons; (C) information of lower quality or having authors with questionable credentials, but that still might be useful to a library patron if nothing else were available or if the patron were doing comprehensive research; and (D) sites inappropriate for children.

Of the 204 sites in the sample, Lipow deemed only one, CyberIron Bodybuilding and Powerlifting, to be inappropriate for

[120] *American Library Ass'n v. U.S.*, 201 F. Supp. 2d at 445. The district court gave numerous examples of such wrongly blocked sites (see the Introduction, pages 3-4).

[121] The district court decision mentions another librarian, Michael Ryan, who reviewed a list of 204 sites that Edelman forwarded to him to evaluate "their appropriateness and usefulness in a library setting." The court said that both Ryan's and Lipow's evaluations were not statistically relevant because the sites they reviewed weren't randomly selected, but that nevertheless, the testimony of both librarians "established that many of the erroneously blocked sites that Edelman identified would be useful and appropriate sources of information for library patrons." 201 F. Supp. 2d at 444 n.17.

children. Her 49 category A sites included the Willis-Knighton Cancer Center Department of Radiation Oncology and a guide to Internet searching. Her 70 category B sites included a Southern California animal rescue organization and the Southern Alberta Fly Fishing Outfitters. In category C, she placed 74 sites, including one offering menstruation information but not authored by an expert, and another advertising a Manhattan podiatry group. Lipow concluded that virtually all of the sites in her sample had been wrongly blocked.

Report of Defendants' Expert Cory Finnell (Oct. 15, 2001)

Cory Finnell of Certus Consulting Group evaluated the filters used by public libraries in Tacoma, Washington, Westerville, Ohio, and Greenville, South Carolina by examining their usage logs. Finnell believed this method was more accurate than many earlier studies because it was based on Web sites that library patrons actually sought rather than sites that researchers thought they would seek. However, Finnell acknowledged that his results could be skewed because library patrons, knowing that filters were installed, might have refrained from seeking controversial sites.

Finnell collected Tacoma's Cyber Patrol usage logs for August 2001;Westerville's WebSENSE logs for October 1-3, 2001; and Greenville's N2H2 logs for August 2-15, 2001. He computed the overblocking rate for each of the filters by, first, reducing each blocked Web page listed in the logs to the host that contained the page. Thus, for example, if the log showed blocked requests for www.fepproject.org/issues/internet.html, www.fepproject.org/issues/sexandcens.html, and www.fepproject.org/news/news.html, Finnell would reduce all three requests to www.fepproject.org. This meant that Finnell was undercounting the actual number of blocked pages.

Second, he examined the default page of each blocked host and sometimes a sample of the host's other pages (although not necessarily the pages that the library patrons had tried to visit), to determine whether the pages' content was consistent with the filter's blocking criteria. Then, for each filter, he computed overblocking as the percentage of incorrect blocks—what Paul Resnick and his colleagues term the "blocked-sites overblock rate."[122] Finally, Finnell checked to see whether any of the incorrect blocks had been corrected in newer versions of the filters' block lists, and calculated separate figures that took these corrections into account. He computed underblocking rates for WebSENSE and N2H2 the same way, arriving at an "unblocked-sites underblock rate," to use Resnick's terminology.

Finnell determined that for Tacoma's Cyber Patrol, 53 out of the 836 blocked hosts were errors, for an overblocking rate of around 6%. For Westerville's WebSENSE, 27 out of the 185 blocks were wrong—an overblocking rate of about 15%—and one out of 159 unblocked hosts should have been blocked, for an underblocking rate of less than 1%. When he took WebSENSE's updated block list into account, the overblocking and underblocking rates dropped to around 13% and 0%. Finally, he decided that 154 out of the 1,674 hosts that Greenville's N2H2 blocked were incorrect, for an overblocking rate of about 9%; and three of the 254 unblocked hosts should have been blocked, for an underblocking rate of around 1%. Taking N2H2's updates into account, he reduced their overblocking and underblocking rates to about 5% and less than 1% respectively.

In a rebuttal report, Geoffrey Nunberg harshly criticized Finnell's methods, especially his decision to reduce the individual page requests in the usage logs to the hosts that contain them. Nunberg pointed out that treating multiple requests for pages on a single host as

[122] See page 45 for a description of Resnick's article.

a single request distorts the test results because whether a host is requested one time or 40 times, it will only be counted once for the purposes of computing over- and underblocking. Numerous different pages on the wrongly blocked hosts were requested, producing actual overblocking rates for the Tacoma and Westerville filters of more than 50%.[123]

Nunberg also noted that Finnell did not specify how many raters he used, how they were trained, or what was done if they disagreed. He pointed out that many of the sites in the Greenville logs that Finnell classified as "offensive" were in fact "innocuous"—for example, a company that sells Internet retailing software packages, an Icelandic Internet service provider, and The *Journal of Contemporary Obituaries*. This led Nunberg to doubt that Finnell examined all of the sites that he claimed to have rated. Finally, Nunberg criticized Finnell's decision to correct the original overblocking and underblocking figures by using the filter manufacturers' updated block lists because although updated lists may correct some errors, they are liable to introduce others. Accounting for these misclassifications, Nunberg found the overblocking rate for Greenville's N2H2 filter was at least 20%—twice what Finnell had calculated.

Finnell's method of calculating overblocking, as the percentage of a filter's blocks that are incorrect, is also problematic. As Resnick *et al.* explained, this figure does not indicate the degree to which a filter limits library patrons' access to particular kinds of information. Even if most of a filter's blocks are correct, it could still wrongly block an unacceptable percentage of sites of a particular kind, such as health education.

His method of computing underblocking, as the percentage of unblocked sites that should have been blocked, is even more deeply flawed. The problem with this measure is that the more "innocuous" Web sites that are included in the test set, the lower the underblocking rate will be. For example, imagine a filter that is incapable of blocking anything. If the filter is evaluated using a test set comprised of one "offensive" site and 99 "innocuous" sites, the underblocking rate, according to Finnell's method, would be only 1%. Since it is likely that most of the library patrons in Finnell's study were not searching for pornography, the vast majority of the unblocked sites in the usage logs were likely "innocuous." As a result, the filters' underblocking rates, computed using Finnell's method, were likely to be low regardless of how badly the filters actually performed.

eTesting Labs, *Updated Web Content Filtering Software Comparison* (Report prepared under contract from the U.S. Department of Justice, Oct. 2001)

The Department of Justice (DOJ) commissioned eTesting Labs to evaluate five filters according to their ability to block images that meet the "harmful to minors" definition in the CIPA law. The researchers, led by defendants' expert Chris Lemmons,[124] also assessed the filters' mistaken blocking of "acceptable" content.

Lemmons began by compiling a list of 197 "objectionable" sites that he thought pornographic and 99 sites that he deemed "acceptable" but potentially confusing to filters. He collected "objectionable" sites by entering the phrase "free adult sex" into a popular search engine, "randomly" visiting some of the sites that were returned by the search, and then placing on the objectionable list those sites that he believed met the DOJ's criteria. He then surfed to other "objectionable" sites by following hyperlinks, and added some of these to the list. Finally, he extracted additional pornography-related keywords from the ob-

[123] *Expert Rebuttal Report of Geoffrey Nunberg* in *American Library Ass'n v. United States*, 19-20.

[124] As identified by the district court, 201 F. Supp. 2d at 437. The filters tested by DOJ were SmartFilter 3.01; Cyber Patrol for Education 6.0; WebSENSE Enterprise 4.3.0; N2H2 Internet Filtering, version not specified; and FoolProof SafeServer, version not specified.

jectionable sites already collected, entered the keywords into the search engine, and added some of the resulting sites to the list. He used a similar combination of searches, surfing, and keywords to compile the list of "acceptable" sites.

As Resnick *et al.* point out, this method of collecting sites is not repeatable and is subject to bias. Although Lemmons claimed to have "randomly" selected the sites on the "objectionable" and "acceptable" lists, his samples were not statistically random but were influenced by the sites and hyperlinks that caught his and fellow researchers' attention while they were surfing the Web. The district court leveled a similar criticism: the selection method "is neither random nor does it necessarily approximate the universe of Web pages that library patrons visit."[125]

The DOJ specified which settings should be used for each filter. Since none of the filters had settings that matched CIPA's definitions, the DOJ picked the settings that it thought most closely matched: for SmartFilter, the "extreme/obscene/violent" and "sex" categories; for Cyber Patrol, "adult/sexually explicit"; for WebSENSE, the "sex" subcategory of "adult materials"; for SafeServer, "pornography"; and for N2H2, "pornography," with exceptions for sites categorized as "education," "history," "medical," and "text/spoken only."

After testing the filters against the two lists of sites, Lemmons computed the percent of "objectionable" sites that each filter blocked. He found that N2H2, SmartFilter, and WebSENSE blocked more than 90% of the "objectionable" sites, while Cyber Patrol and SafeServer blocked 83% and 76% respectively.

As for overblocking, he found that WebSENSE did not block any of the "acceptable" sites, while N2H2 blocked only one. Cyber Patrol, SmartFilter, and SafeServer blocked 6%, 7%, and 9% respectively. Examples of incorrectly blocked sites included an STD information site for teenagers, a list of Web resources for lesbians, the Web site of a sexual abstinence education program, an online condom store, the Web site of Schick and Wilkinson brand razors, a list of Web resources aimed at African-American women, and a site discussing the Bible's position on homosexuality.

Plaintiffs' expert Geoffrey Nunberg leveled numerous criticisms at the eTesting Labs report. He contended that the results were unrealistic because the researchers did not make any effort to ensure that different types of sites appeared on their lists in the same proportions as they do on the Web. Like other commenters, Nunberg also chastised eTesting for not specifying what standards its raters used to judge sites as objectionable or acceptable, how many raters were used, and how difficult-to-classify sites were handled.[126]

Rebuttal Report of Plaintiffs' Expert Benjamin Edelman (Nov. 30, 2001)

Edelman elaborated on the flaws of Internet filters and leveled specific criticisms against the studies of eTesting Labs and Cory Finnell.

The first flaw was filters' inability to block content from sources outside the Web, such as email and streaming video. Edelman tested the same four filters that he examined for his initial report—Cyber Patrol, N2H2, SmartFilter, and WebSENSE—and found that none stopped him from receiving sexually explicit images through email. He also found that although the filters blocked access to most of the Web sites he visited containing links to sexually explicit videos, he could view those videos if he typed their URLs directly into a video player program.

Like Nunberg, Edelman criticized eTesting Labs's decision to focus on sites that they deemed likely to confuse filters. He argued that this method significantly understates overblocking because it excludes whole cat-

[125] *American Library Ass'n v. U.S.*, 201 F. Supp. 2d at 437-48.

[126] *Expert Rebuttal Report of Geoffrey Nunberg,* 1-11.

egories of sites that filters wrongly block for no apparent reason. Examples from Edelman's test set included the Southern Alberta Fly Fishing Outfitters, blocked by N2H2 and WebSENSE, and Action for Police Accountability, blocked by N2H2, SmartFilter, Cyber Patrol, and WebSENSE.

Also like Nunberg, Edelman contended that because eTesting used a search engine to compile a list of sites to test, its results were biased by the search engine's method of ranking Web pages. Search engine results are skewed toward popular sites, especially among the first few hundred hits. Since Internet filters use methods similar to search engines to compile their

The more "innocuous" Web sites that are included in the test set, the lower the underblocking rate will be.

block lists, they are likely better at blocking popular sexually explicit sites than they are at blocking obscure ones. Consequently, if eTesting collected most of its test sites from the first few hundred hits returned by Google, its results would overstate filters' effectiveness because its test set would be comprised of just the sort of sites that filters are best at blocking.

To test this theory, Edelman searched Google for "free adult sex" and collected 795 results. He then tested these sites against the four filters he had examined in his initial report and found that they were better at blocking the first hundred than subsequent results. On average, the filters blocked 86% of hits 1-100, but only 79% of hits 701-795. In fact, the filters only performed as well as eTesting had claimed on the first 50 hits and significantly worse thereafter. Edelman concluded that, despite its claims to the contrary, eTesting generally did not examine search results beyond the first 50 hits.

Finally, Edelman criticized Finnell for adjusting the results of his analysis using updated versions of the filters' block lists because although the updated lists might have corrected some errors, they were liable to introduce new ones. It was wrong, he argued, for Finnell to assume that just because filter manufacturers had corrected some errors, the overall performance of filters had improved.

Supplemental Report of Plaintiffs' Expert Benjamin Edelman (Mar. 13, 2002)

Several months after submitting his initial report, Edelman retested three of the four filters he had initially examined—N2H2, Cyber Patrol, and WebSENSE—to see whether they continued to block the sites they had blocked in his initial study. He found that N2H2 continued to block 55% of these sites, while WebSENSE continued to block 76%. By contrast, Cyber Patrol only continued to block 7%. That is, Cyber Patrol had unblocked 93% of the sites on Edelman's list. The district court found that this behavior constituted an admission that thousands of pages had been wrongly blocked.[127]

Two Reports by Peacefire

"More Sites Found Blocked by Cyber Patrol" (Jan. 2002)

Peacefire found numerous Web sites wrongly blocked by Cyber Patrol. These included the religious organizations Catholic Students Association and Hillel of Silicon Valley; the youth organizations Aleh (which provides medical care to disabled children in Israel), Acorn Community Enterprises, and the Variety Club of Queensland; the environmental and animal rights groups Universal Ecology Foundation, Columbia River Eco-Law Enforcement, and South Carolina Awareness and Rescue for Equines; the gay and lesbian issue sites Parents, Families, and Friends of Lesbians and Gays and Lesbian and Gay Psychotherapy

[127] *American Library Ass'n v. U.S.*, 201 F. Supp. 2d at 443.

of Los Angeles; and other sites including Adoption Links Worldwide, and First Day of School America (a site promoting parental involvement in schools). All were blocked as "sexually explicit."

Peacefire concluded that, given these errors, Cyber Patrol's original claim that all sites on its block list were hand-reviewed was not credible. It noted that the claim "no longer appears on their Web page."

"WebSENSE Examined" (2002)

Peacefire reported that WebSENSE wrongly blocked, as "sex," KinderGarten.org (an organization funding free vaccinations for children in India); the Navarra, Spain chapter of the Red Cross; and Keep Nacogdoches Beautiful (a site devoted to cleaning up Nacogdoches, Texas), among others. It blocked Autism Behavioural Intervention Queensland, as "gambling," and the Shoah Project (a Holocaust remembrance site), as "racism/hate," possibly because it includes the names of prominent Holocaust deniers.

Peacefire also recounted an experiment it undertook to determine whether WebSENSE is biased in favor of large, well-known organizations. It took anti-gay quotes from the Web sites of four prominent groups with homophobic viewpoints,[128] and posted them to four small sites that were hosted at no cost by companies like GeoCities. It then used anonymous email accounts to submit the free pages to WebSENSE's manufacturer for review without revealing the sources of the quotes. In response, the manufacturer agreed to block three of the sites as "hate speech," but when it was told that the quotes on the small sites came from prominent conservative sites that its filter did not block, it refused to block the prominent sites.

[128] The groups were: the Family Research Council, Focus on the Family, the Official Dr. Laura Web Page, and Concerned Women for America. For details of the experiment and the quotes used, see www.peacefire.org/BaitAndSwitch/ (visited 2/16/06).

Two Reports by Seth Finkelstein

"BESS vs. Image Search Engines" (Mar. 2002)

This short article documented Bess's wholesale blocking of popular image search engines that can be used to find both "objectionable" and "unobjectionable" content. With only its "pornography," "nudity," or "swimsuit" categories activated, Bess blocked Google, Lycos, Ditto.com, AltaVista, and AlltheWeb image searches.

Bess now categorizes these sites as "search" or "visual search engine."[129] Because of their ability to display both pornographic and nonpornographic thumbnails, image search engines continue to cause difficulty for filters.

"BESS's Secret Loophole" (Aug. 2001, revised and updated Nov. 2002)

This article describes how Bess, like other popular filters, blocks anonymization, translation, HTML validation, and "dialectizer" sites that contain no "objectionable" material simply because, as a side effect of their operation, the sites can be used to circumvent filters. That is, by routing requests through these sites, users can hide the requests from filters.

Thus, Bess blocked the anonymization sites Anonymizer.com, IDzap, and Megaproxy; the language translation sites Google Translate, Babel Fish, and Dictionary.com translation service; the HTML validation services Anybrowser.com and Delorie Software Web Page Purifier; and the humorous "dialectizer" sites "Smurf the Web!" and "Jar-Jargonizer." At the time Finkelstein published this article, Bess's blocking of these so-called "loophole" sites was completely undocumented and could not be disabled. That has since changed, but Bess's manufacturer warns that "unless this category [*i.e.* loophole sites] is selected, the system's

[129] Bess's categorizations were verified using the BESS URL Checker located at database.n2h2.com/cgi-perl/catrpt.pl (visited 6/30/05).

Internet Content Filtering protection can be compromised."[130]

The Kaiser Family Foundation: Blocking of Health Information

Caroline Richardson, *et al.*, "Does Pornography-Blocking Software Block Access to Health Information on the Internet?" 288:22 *Journal of the American Medical Association* 2887-94 (Dec. 11, 2002); summarized in Victoria Rideout, Caroline Richardson, & Paul Resnick, *See No Evil: How Internet Filters Affect the Search for Online Health Information* (Kaiser Family Foundation, Dec. 2002)

In response to studies showing that adolescents are increasingly using the Internet to find health information, researchers under contract with the Henry J. Kaiser Family Foundation investigated the degree to which filters designed to block pornography also prevent teenagers from accessing information on several health topics. They tested six filters commonly used in schools and libraries, and one designed for home use,[131] against a list of health sites that they believed would be of interest to teenagers. They also tested the filters' efficiency at blocking pornographic sites.

The researchers collected their list of sites both by simulating adolescents' search habits and by consulting the health site recommendations for teenagers in the online directories of Yahoo! and Google. To simulate teen searching habits, they chose five categories of content: "(1) health topics unrelated to sex (*e.g.* diabetes); (2) health topics involving sexual body parts, but not sex-related (*e.g.* breast cancer); (3) health topics related to sex (for example, pregnancy prevention); (4) controversial health topics (*e.g.* abortion); and (5) pornography." For each category, they chose six frequently used search terms from the search engine logs of Overture.com and Excite and entered them into six search engines popular among teenagers. The simulation of teenagers' search behavior yielded 3,987 sites, of which the raters concluded that 2,467 contained health information, 516 contained pornography, and 1,004 contained neither. The search of Yahoo! and Google online directories produced 586 health sites recommended for teens.

To evaluate the sites they collected, the researchers employed two raters who each explored 60% of the sites and assigned them ratings of "health information," "pornography," or "other." In an attempt to be consistent with U.S. obscenity law, they considered a site pornographic if it depicted genitals or a sexual act, if it seemed designed to appeal to a prurient interest, and if it did not appear to be educational or scientific.[132]

The school and library filters were tested using three different levels of blocking. The "least restrictive" configuration generally was designed to block only pornography. The "intermediate" setting was supposed to block sites dealing with illegal drugs, nudity, and weapons in addition to pornography. The third and most restrictive configuration included all of the categories that "might plausibly be blocked" in a school or library. For AOL Parental Controls, the researchers tested two configurations: its moderately restrictive configuration for mature teens and its very restrictive configuration for young teens.

The results overall showed, first, that how a filter is configured has a big impact on the number of health information sites that are erroneously blocked; and second, that using a more restrictive configuration does little to

[130] See the description of the "P2P/loopholes" category at www.securecomputing.com/index.cfm?skey=1379 (visited 3/11/06).

[131] The six filters commonly used in schools or libraries were: SmartFilter 3.0.1; 8e6 Filter 4.5; WebSENSE 4.3.1; Cyber Patrol SuperScout 4.1.0.8; Symantec Web Security 2.0; and N2H2 Filter 2.1.4. The filter commonly used in homes was America Online Parental Controls.

[132] On the U.S. Supreme Court's standard for illegal "obscenity," see the Introduction, page 2; see also Free Expression Policy Project, *Fact Sheet on Sex and Censorship* (n.d.). Pornography is not a legal term, and is not the same as obscenity under the law.

improve a filter's ability to block pornography, while dramatically increasing the number of health sites that are wrongly blocked.

On their least restrictive settings, the six filters common in schools and libraries blocked an average of 87% of the pornographic sites and of 1.4%, overall, of the health information sites. When filtering was increased to the "intermediate" level, the blocking rate for pornography only increased to 90%, while the blocking rate for health information increased to over 5%. At the most restrictive configuration, the blocking rate for pornography inched up to 91% while the blocking rate for health information reached 24%. The researchers observed similar results for AOL Parental Controls.

Examples of erroneous blocks on the filters' least restrictive settings (i.e., ostensibly only blocking pornography) included a health information site for gays and lesbians, a sex education site run by Columbia University, a site discussing sexually transmitted diseases run by the National Institute of Allergy and Infectious Diseases, and an online condom store. On the intermediate blocking level, the errors, according to the authors, included a lung cancer information site, a directory of suicide prevention telephone hotlines, Planned Parenthood, and a Spanish-language herpes information site sponsored by the Children's Hospital in Boston. On the most restrictive settings, the blocks that the authors considered erroneous included the American Academy of Pediatrics' "Woman's Guide to Breastfeeding," the *Journal of the American Medical Association*'s Women's Health STD Information Center, and the sites of the Depo Provera birth control company, the National Campaign to Prevent Teen Pregnancy, the American Society of Clinical Oncology, and the U.S. Center for Disease Control's Diabetes Public Health Resources.

Since the average overblocking rate at the least restrictive configurations was just 1.4% for all health sites, the researchers concluded that filtering products set at their least restrictive settings are only a minor impediment to teens' ability to find information on most health topics, especially compared to other factors such as "spelling errors, limited search skills, and [the] uneven quality of search engines."[133] But the 1.4% error rate may be misleading. Some of the blocked sites might have had information not available elsewhere; and even a seemingly low error rate, when applied to the Internet, could amount to thousands of wrongly blocked health sites.

Moreover, even on their least restrictive settings, the filters erroneously blocked roughly 10% of the nonpornographic sites returned by searches on controversial topics such as "safe sex," "condom," and "gay." With the intermediate configuration, the blocking rate for the nonpornographic sites on these topics was 20-25%, and on the most restrictive configuration, that figure rose to 50-60%.

In addition to computing the average blocking rate at each of three levels, the researchers calculated the percentage of sites at each level that were blocked by at least one filter. These figures were substantially higher than the average blocking rates. For example, at the least restrictive blocking level, 5% of health information sites were blocked by at least one filter, and on the most restrictive, that number was 63%. 33% of the nonpornographic health sites returned by a search for the term "safe sex" were blocked by at least one filter even at the least restrictive blocking level, and 91% were blocked by at least one filter at the most restrictive level. Although these figures don't indicate how any of the individual filters performed, the disparities between average and the cumulative blocking rates show how greatly filters disagree about exactly what should be blocked.

[133] Rideout *et al.*, Exec. Summary, 12.

In light of their findings about the importance of a filter's configuration, the researchers argue that the choice of settings should not be left to network administrators and should be considered a policy decision that is at least as important as the decision to install Internet filters in the first place.

Reactions to this study varied. The Kaiser Family Foundation's press release began: "The Internet filters most frequently used by schools and libraries can effectively block pornography without significantly impeding access to online health information—but only if they aren't set at their most restrictive levels."[134] The Foundation's *Daily Reproductive Health Report*, however, cited articles in the *New York Times* and *Wall Street Journal* that emphasized: "Internet filters intended to block access to pornography on school and library-based computers often block access to sites containing information on sexual health … Among the sites blocked were a Centers for Disease Control site on sexually transmitted diseases; a Food and Drug Administration site on birth control failure rates; and a Princeton University site on emergency contraception." [135] One commentary described the study's more dramatic findings—63% blocking of general health sites and 91% blocking of sexual health sites by at least one filter— in a way that suggested these were across-the-board findings for searches of "sexually related materials."[136]

[134] Kaiser Family Foundation news release (Dec. 10, 2002), www.kff.org/entmedia/upload/See-No-Evil-How-Internet-Filters-Affect-the-Search-for-Online-Health-Information-News-Release.pdf (visited 3/11/06).

[135] Kaiser Family Foundation, *Daily Reproductive Health Report* (Dec. 11, 2002), www.kaisernetwork.org/daily_reports/rep_index.cfm?hint=2&DR_ID=15033 (visited 3/28/05).

[136] Paul Jaeger & Charles McClure, "Potential Legal Challenges to the Application of the Children's Internet Protection Act in Public Libraries," *First Monday* (Jan. 16, 2004). The description is inaccurate for two reasons: first, the results that it quotes were only obtained at the most restrictive blocking level when the filters were configured to block several other categories of content in addition to "sexually related materials"; and second, the figures are cumulative, and don't describe the performance of any single filter.

Two Studies by the Berkman Center for Internet and Society

Benjamin Edelman, "Web Sites Sharing IP Addresses: Prevalence and Significance" (Feb. 2003)

About a year after his testimony in the CIPA case, Edelman published a report on IP address filtering. When someone attempts to access a Web site, the site's domain name is first converted into a numerical Internet Protocol (or IP) address. These numbers identify the server that hosts the site. Current technology enables a single server with a single IP address to host more than one Web site.

This creates problems for Internet filters because some filtering works by blocking the IP address of the server instead of blocking the domain name of the "offending" site. To gauge the scope of this potential overblocking, Edelman sought to find out what percentage of the sites on the Web share their server, and therefore their IP addresses, with other sites.

Edelman collected the IP addresses of more than 20 million active Web sites ending in ".com," ".net," and ".org," and found that IP sharing was the rule, not the exception. The great majority—87%—of the sites shared their servers and IP addresses with at least one other site. 82% of the sites resided on servers that hosted at least five sites; 75% resided on servers that hosted at least 20; and 70% resided on servers that hosted at least 50. Often, the sites sharing an address had nothing to do with one another. For example, a server with the IP address 206.168.98.228 hosted both www.phone-sex-jobs.com and www.christian-newswatch.com.

Despite this showing that filtering based on IP addresses inevitably causes overblocking, Edelman noted that the technique is still widely used because it is less expensive than filtering based on domain names. He does not identify which products use IP-based filtering.

Benjamin Edelman, "Empirical Analysis of Google SafeSearch" (Apr. 2003)

A second study by Edelman concerned the Google search engine feature SafeSearch, which screens for explicit sexual content. Google says that SafeSearch primarily uses an automated system instead of human reviewers, and it readily admits that its system is inaccurate.[137] Although SafeSearch does not block users from accessing particular sites, its filtering of search results can prevent them from finding or even knowing about whole categories of content.

Edelman entered approximately 2,500 search terms on a wide variety of topics, chosen in an ad hoc fashion, into Google's Web search and compared the results of unfiltered searches to those of searches conducted with SafeSearch. He found a total of 15,796 distinct URLs omitted from SafeSearch; in some instances, the entire corresponding site was excluded. It is not clear how many of the 15,796 Edelman considered errors; he wrote that his "[r]eporting focuses on URLs likely to be wrongly omitted from SafeSearch, *i.e.* omitted inconsistent with stated blocking criteria" (that is, "explicit sexual content").

Among the many pages without any apparent sexual content that SafeSearch eliminated were: U.S. government sites (congress.gov, thomas.loc.gov, shuttle.nasa.gov); sites operated by other governments (Hong Kong Department of Justice, Canadian Northwest Territories Minister of Justice, Israeli Prime Minister's Office); political sites (Vermont Republican Party, Stonewall Democrats of Austin, Texas); news reports (from the *New York Times*, the BBC, *C/net* news, the *Washington Post*, and *Wired*); educational institutions (a chemistry class at Middlebury College, Vietnam War materials at U.C.-Berkeley, and the University of Baltimore Law School); and religious sites (the Biblical Studies Foundation, Modern Literal Bible, Kosher for Passover). Edelman observed that some of these sites "seemed to be blocked based on ambiguous words in their titles (like Hardcore Visual Basic Programming)," but "most lacked any indication as to the rationale for exclusion."

Edelman also recorded the frequency of blocking when search results were unrelated to sex. In a search for "American newspapers of national scope," SafeSearch excluded sites from among the top ten results 54% of time. It excluded sites from among the top ten results 23% of the time for searches on "American presidents," 20% of the time for searches on "most selective colleges and universities," and 16% of the time for searches on "American states and state capitals." Reviewing some of the excluded sites, Edelman found that most were not sexually explicit.

For searches on more controversial topics such as sexual health, pornography, and gay rights, SafeSearch's blocking seemed to be arbitrary. For example, in response to a search for "sexuality," SafeSearch listed the Society for the Scientific Study of Sexuality, but excluded the peer-reviewed *Electronic Journal of Human Sexuality*. In response to a search for "pornography," it included a National Academy of Sciences report on Internet pornography, but omitted a book on the topic published by the National Academies Press.

Even at their narrowest settings, filters block much more than CIPA requires.

Despite Google's claim that SafeSearch is only designed to block sexually explicit material, Edelman determined that it also excluded other controversial material. It omitted several sites advocating illegal drugs but also the White House Office of National Drug Control Policy. It also excluded gambling

[137] SafeSearch is described in two sections of Google's help site, www.google.com/help/customize.html#safe and www.google.com/safesearch_help.html (visited 4/1/05).

sites; online term paper mills; sites that discuss pornography without exhibiting it such as the Pittsburgh Coalition Against Pornography; companies making Internet filtering software; and Edelman's own reports on Internet filtering in China and Saudi Arabia.

Edelman discovered a quirk in SafeSearch's design that might explain some of its overblocking. When Google explores the Internet, it makes a copy of the Web pages that it encounters and stores them in a cache. Sometimes, though, the software fails to record a site in the cache—for example, when a Web site operator indicates that she doesn't want the site to be cached or when a site is temporarily unavailable. Edelman learned, by consulting with Google staff, that SafeSearch excludes all sites that are missing from the cache even though their absence has nothing to do with their content. Out of his list of sites omitted by SafeSearch, he discovered that 27% were missing from Google's cache. This suggests that many sites excluded by SafeSearch are blocked not because they meet Google's blocking criterion, but simply because of SafeSearch's design.

Electronic Frontier Foundation/ Online Policy Group Study

Internet Blocking in Public Schools: A Study on Internet Access in Educational Institutions (June 26, 2003)

This study had two main purposes: to measure whether filters block material relevant to state-mandated school curricula, and to determine how well filters perform schools' obligations, under CIPA, to block visual images that are "obscene," child pornography, or "harmful to minors."

The researchers conducted Web searches for topics taken directly from the K-12 curricula of California, Massachusetts, and North Carolina; then tested the two Internet filters most popular in schools—Bess and SurfControl—against the resulting sites. Retrieving up to 50 results from each search, they produced a list of nearly a million relevant Web pages, including duplicates.

For Bess, they used an existing installation at an unnamed public high school, and did not know which categories were activated, but "speculated" that they were "similar to those of many other schools." On the other hand, they tested SurfControl against a "test tool" which a company representative assured them provided "the same results as the product sold to schools."[138] They tested SurfControl on its "core" configuration set to block 10 categories ("adult/sexually explicit", "chat," "criminal skills," "drugs, alcohol & tobacco," "gambling," "hacking," "hate speech," "violence," "weapons," and "Web-based email"), as well as its "core plus" (the 10 core categories plus "glamour & intimate apparel," "personals & dating," and "sex education"); and an "all" configuration that blocked all SurfControl categories.

The researchers did not examine every Web page that they collected to determine whether or not it was correctly blocked or unblocked. Instead, they examined random samples of approximately 300 sites each. The report does not specify how many raters evaluated the sites or whether their ratings agreed.

For the first measure of performance, the researchers concluded, not surprisingly, that the vast majority of blocked sites did not need to be blocked in order to comply with CIPA. Out of the more than 31,000 pages that Bess blocked, only 1%, they thought, fit CIPA's definitions of obscenity, child pornography, or "harmful to minors" images. Even expanding CIPA's criteria to include nonvisual material, the researchers said that only 2% needed to be blocked.[139]

[138] *Internet Blocking in Public Schools*, 15.

[139] Most of the pages blocked by Bess were not classified as "pornography" or "sex," but fell into categories like "free pages" and "electronic commerce." Among the blocked pages that Bess classified as "pornography" or "sex," the researchers concluded that only 6% fit CIPA's criteria.

As for SurfControl, the researchers determined that out of 3,522 pages blocked using the "core plus" configuration, only 3% fit CIPA's criteria (5% if text and not just images are included). Of the blocked pages that SurfControl classified as "adult/sexually explicit," 6% fit CIPA's criteria, in the researchers' judgment.

The second measure of performance, the percentage of curriculum-relevant search results that each filter blocked, was reported both overall and by curriculum topic. Some of these sites were arguably within one or more of the filters' broad blocking categories. For example, both filters blocked five Web pages associated with a curriculum topic on the U.S. Populist movement. The five pages all contained information on National Socialism, which was probably blocked as "hate/discrimination" by N2H2 and as "hate speech" by SurfControl.

Among the many sites that the researchers thought Bess wrongly blocked, both because they were relevant to school curricula and because they had no visual depictions that would require blocking under CIPA were: Heroines of the Revolutionary War, a site created by a librarian for the use of 4th grade students (blocked as "recreation/entertainment"); Poetry-making and Policy-making (miscategorized as "pornography"); Maryland Mental Health Online and Electrical & Electronics, Ohm's Law, Formulas & Equations (both miscategorized as "free pages"); and Abraham Lincoln Inaugural Address (miscategorized as "recreation/entertainment").

Examples of sites the authors said were wrongly blocked by SurfControl were: Social Changes in Great Britain Before 1815 (mischaracterized as "glamour and intimate apparel"); Punctuation Primer (blocked as "adult/sexually explicit"—the authors suggest that "perhaps 'period,' as in menstruation, was the trigger"[140]); Responding to Arguments Against Comprehensive Sexuality Education and Oral Contraceptive Pill (both categorized correctly as "sex education," but inappropriately filtered because they had "no visual depictions that would require blocking under CIPA"); Mount Olive Township Fraternal Order of Police: Mistreatment of the Elderly (miscategorized as "adult/sexually explicit"; the page mentions sexual assault on elderly persons); and History, Science and Consequences of the Atomic Bomb (miscategorized as "weapons").

Turning to how well the filters' performance matched the manufacturers' blocking criteria, the study found that Bess misclassified 30% of the sites that it blocked, while SurfControl misclassified 55-66%. The researchers also report a number of instances where the filters did not block clearly pornographic sites.

This study demonstrates two points about filtering in schools. First, even at their narrowest settings, filters block much more than CIPA requires. Second, when schools go beyond CIPA's requirements, to activate such filter categories as weapons, drugs, gambling, hate speech, and electronic commerce, they end up blocking a great deal of material on school curriculum subjects.

American Rifleman

"Internet Filter Software Blocks Only Pro-Gun Sites" (Nov. 2003)

This short article reported that the Symantec Internet Security filter blocks National Rifle Association sites under certain configurations, but does not block the Web site of the Brady Center, which favors gun control. A Slashdot blogger reporting on this news did a follow-up test which confirmed that even the NRA's Institute for Legislative Action was blocked, while anti-gun sites including"Good Bye Guns" were not.[141]

[140] *Internet Blocking in Public Schools*, 26.

[141] "Symantec Says No to Pro-Gun Sites" (Nov. 2, 2003), yro.slashdot.org/article.pl?sid=03/11/02/1729239&mode=thread&tid=103&tid=153&tid=99 (visited 2/10/06).

Colorado State Library

Carson Block, *A Comparison of Some Free Internet Content Filters and Filtering Methods* (Jan. 2004)

The Colorado State Library tested six filters against 25 search terms to learn whether they blocked materials in legitimate library-selected research databases such as EBSCO, the Denver Public Library's Western History Collection, and Access Colorado Library Information Network Best Websites. Four of the filters were either free or bundled at no additional cost with resources such as Google.com or Internet Explorer; and two were "for-pay filters" (Cyber Patrol and SmartFilter). [142]

Of the free filters, We-Blocker blocked research database materials when the search terms "incest," "pierce," "transsexual," "whipped," "teen," and "Wicca" were used. Examples included health information on body piercing from Black Entertainment Television; dictionary definitions of "Wicca"; and a review of the movie "Whipped" from *Rolling Stone* magazine. "The Family Browser" was more restrictive, blocking legitimate research materials when these terms as well as the following others were used: "cum," "Satan," "stud," "tattoo," "witchcraft," "breast," "Nazi," "AIDS," "beaver," "gun," "model," and "pagan." Among the questionable blocks was a State of Colorado wildlife site—because of the word "beaver."

Content Advisor was by far the most restrictive, blocking access to materials using any of the 25 terms, regardless of how innocent their context. This was because Content Advisor is essentially a whitelist: it only allows access to sites that have voluntarily self-rated.

Cyber Patrol blocked research database materials containing the words "cum," "gun," "incest," "model," "Nazi," "stud," "bomb," "pot," and "teen." For example, it blocked as "adult/sexually explicit" a list of magazine articles containing physical and mental health information for victims of incest; and, as "glamour and intimate apparel," sites having nothing to do with glamour or intimate apparel (the trigger word was "model").

SmartFilter did not block materials in any of the three library databases—probably, according to the author, because it "is configured to work with the Fort Collins Public Library."[143]

OpenNet Initiative: Advisory 001

Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran (May 3, 2004)

OpenNet Initiative is a joint project of the University of Cambridge, England, the Munk Centre for International Studies at the University of Toronto, and the Berkman Center at Harvard. Its aim is to "excavate, expose and analyze filtering and surveillance practices in a credible and non-partisan fashion." Although its research focuses on Internet filtering by foreign governments such as Saudi Arabia and China, one of its studies should be mentioned here because it involved a use of filtering technology by the U.S. government.

In 2003, the U.S. government's International Broadcasting Bureau (the IBB) created a plan to give Internet surfers in China and Iran the ability to bypass their nations' notoriously restrictive blocks on Web sites such as BBC News, MIT, and Amnesty International. But the IBB used technology that, as journalist Declan McCullagh reported, prevents surfers "from visiting Web addresses that include a peculiar list of verboten key-

[142] The free filters were WINnocence (free software from Peacefire which has just three sites on its block list—*Playboy, Hustler*, and www.sex.com); We-Blocker, The Family Browser, and Content Advisor (which is built into many browsers, including Internet Explorer).

[143] Block, Exec. Summary, 9.

words. The list includes 'ass' (which inadvertently bans usembassy.state.gov), 'breast' (breastcancer.com), 'hot' (hotmail.com and hotels.com), 'pic' (epic.noaa.gov) and 'teen' (teens.drugabuse.gov)."[144]

The technology in question was Anonymizer, Inc.'s built-in anti-pornography filter that included "trigger" keywords. In addition to usembassy.state.gov, according to the OpenNet Initiative report, blocked sites included www.georgebush.com, www.bushwatch.com, www.hotmail.com, hotwired.wired.com, www.teenpregnancy.com, www.tvguide.com, and www.arnold-schwarzenegger.com.

McCullough noted that if the government's filter blocked only hard-core pornography, "few people would object." Instead, the filter revealed a conservative bias that included "gay" in its list of forbidden words—thereby blocking not only sites dealing with gay and lesbian issues but DioceseOfGaylord.org, a Roman Catholic site. He quoted the president of Anonymizer as offering to unblock nonpornographic sites upon request by Chinese or Iranian 'Net surfers, but as saying that "we have never been contacted with a complaint about overbroad blocking."[145]

Rhode Island ACLU

Amy Myrick, *Reader's Block: Internet Censorship in Rhode Island Public Libraries* (Rhode Island Affiliate, American Civil Liberties Union, Apr. 2005)

In the course of a 2004 survey conducted to learn how many Rhode Island libraries were using filters,[146] the ACLU's Rhode Island affiliate also collected evidence of overblocking. Researchers found that the installed WebSENSE filter blocked, among others, the official site of the photographer Robert Mapplethorpe, a men's health site, an interview with actor Peter Sellers on *Playboy's* Web site, and a Google search for "nudism."

Consumer Reports

"Filtering Software: Better, But Still Fallible" (June 2005)

This article begins by asserting that filters are "better at blocking pornography than in recent years," but "our evaluation of 11 products, including the filters built into online services AOL and MSN, found that the software isn't very effective at blocking sites promoting hatred, illegal drugs, or violence." In addition, "as we found in our tests in 2001, the best blockers today tended to block many sites they shouldn't."[147]

The researchers created two lists—one consisting of objectionable sites "that anyone can easily find"; the other of "informational sites to test the filters' ability to discern the objectionable from the merely sensitive." They configured the filters as they thought the parents of a 12-15 year-old would. They found that although filters "keep most, but not all, porn out," the "best porn blockers were heavy-handed against sites about health issues, sex education, civil rights, and politics." Seven products blocked "KeepAndBearArms.com"; four blocked the National Institute on Drug Abuse. KidsNet was the worst, blocking 73% of useful sites.

"Research can be a headache" with filters, the report concluded. "These programs may impede older children doing research for school reports. Seven block the entire results page of a Google or Yahoo search if some links have objectionable words in them." AOL blocked NewsMax, a conservative political site, and Operation Truth, an advocacy site for veterans of the Iraq war.

[144] Declan McCullough, "U.S. Blunders with Keyword Blacklist," *C/net News* (May 3, 2004).

[145] *Id.*

[146] See a summary of the findings in the Introduction, pages 5–6.

[147] Among the 11 filters tested were AOL, KidsNet, CYBERsitter, Norton Internet Security, Safe Eyes, and MSN. The online article did not give a complete list.

Experiences of High School Students Conducting Term Paper Research

Lynn Sorenson Sutton, *Experiences of High School Students Conducting Term Paper Research Using Filtered Internet Access* (PhD dissertation, Graduate School of Wayne State University, 2005)

Lynn Sutton, director of the Wake Forest University undergraduate library, studied the experience of students at a suburban high school using Bess. She focused on two classes—one consisting of 11th grade rhetoric students who were preparing for an advanced placement literature course in their senior year; the other, 10th-12th grade general composition students. Sutton contacted nine teachers who assigned research papers, but only two agreed to have their classes participate. Sutton used group interviews, emails with individual students, review of students' journal entries, and observation of actual research activity to gather data.

The school district's director of technology told Sutton that Bess was being used at the default setting, with an option for staff to adjust the settings at their discretion. The default blocked "adults only," "alcohol," "chat," "drugs" (but not the subcategory drug education), "jokes," and "lingerie."

Sutton reported that students were frustrated, annoyed, and angered by the operation of the filter. A girl preparing a paper on the Motion Picture Association of America's movie rating system was completely unable to do her research on the school's computers. Another girl was blocked from www.cannabis.com and similar sites while researching the legalization of marijuana for medical purposes. A boy was blocked from accessing www.ncaa.org while seeking information about college athletes. Another student researching the subject of book banning was repeatedly blocked when using the search terms "corruption" and "banned."

The students also reported instances of underblocking. The girl who was trying to research the MPAA rating system noted that she accidentally accessed a site offering porn movies, even while a large number of informative sites were blocked. She eventually completed her research on her unfiltered home computer.

Among Sutton's other findings were that the majority of teachers and students did not know that they could ask for the filter to be disabled, or for wrongly blocked sites to be unblocked. The technology director was particularly ignorant of the problems caused by filtering, and out of touch with the situation at the school. As Sutton later told a meeting of the American Association of School Librarians: too often "the technology director just installs the filter. He isn't aware of the problems people are having. And no one ever tells him."[148]

Although the librarians, and some of the teachers, felt that filtering didn't work, their input was not credited during the school's decisionmaking process. During the study, the students offered many alternative suggestions for addressing concerns about unfiltered Internet access, "but sadly, they were never asked for input by their school." The students, she concluded,

> did not dismiss lightly societal concern for sexually explicit materials on school premises. They understood that some, presumably younger, children may need guidance in sorting out "bad" materials on the Internet. But they resented a poorly conceived and disastrously implemented artificial device that prevented them from accessing needed information without any input

[148] As reported in Corey Murray, "Overzealous Filters Hinder Research," *eSchool News Online* (Oct. 13, 2005).

into the decision or any effective way to redress inequity.[149]

Among the drawbacks of this study were its small sample size and limited scope. Sutton notes that this was a mostly white suburban school, most of whose students had Internet access at home. The study group was self-selected and the research was largely anecdotal. Nevertheless, the study gives a vivid sense of the frustrations that filters cause for students.

Computing Which? Magazine

"Software Alone Can't Create a Safe Online Playground" (Aug. 30, 2005)

The British magazine *ComputingWhich?* reported that in its tests of seven popular filters,[150] the software often failed to block pornographic and racist Web sites. Norton Internet Security and Microsoft's MSN Premium performed the worst, with scores of less than 35% across a series of tests. The magazine's editor commented: "Software can help make the Internet a safer environment for children but there's no substitute for parental involvement. Parents need to take an active role in monitoring what their children are looking at online so they don't inadvertently put them at risk."[151]

PamRotella.com: Experiences with iPrism

Pam Rotella, "Internet 'Protection' (CIPA) Filtering Out Political Criticism" (Nov. 22, 2005; updated Nov. 23, 2005)[152]

Pam Rotella publishes a Web site on vegan vegetarianism, nutrition, alternative medicine, and politics. In November 2005, she reported on her blog that she had been blocked from the political satire page PresidentMoron.com at her local library.[153] She received a message that the site was "adult political humor." Off to the side of the computer was a notice that the iPrism filter had been installed in order to comply with CIPA, and that patrons could request that the filter be turned off if they believed that sites had been erroneously blocked. Rotella made the request, and the librarian unblocked this one site for one hour.

Although PresidentMoron.com vigorously criticizes the Bush Administration, it is not sexually explicit. Rotella wondered if "CIPA is being used as a way of blocking political free speech"?

The next day, she returned to the library "and decided to try a few more political sites." None had vulgar language but all were critical of the Bush Administration. Here's what she found:

- www.toostupidtobepresident.com was blocked as "tasteless";
- www.whitehouse.org was blocked as "adult, mature humor";
- www.comedyzine.com was blocked as "adult";
- several other comedy sites were blocked as "mature humor," "adult," or "politics."

Rotella noted, meanwhile, that Rush Limbaugh's site was not blocked.

Further research by FEPP revealed that iPrism is marketed by St. Bernard Software and uses iGuard technology. As of February 2006, it had 65 blocking categories, ranging from "copyright infringement" and "questionable" to "alt/new age," "politics," "religion,"

[149] Sutton, 86-87.

[150] The magazine's press release gave the number as six, but then listed seven: Net Nanny 5.1, AOL 9.0, Cyber Patrol 7, McAfee Internet Security Suite, MSN Premium, Norton Internet Security 2005, and MacOS X Tiger. *Computing Which?* press release, "Software Alone Can't Create a Safe Online Playground" (Aug. 30, 2005).

[151] *Id.* The study was referenced in Bobbie Johnson, "Nanny Software 'Fails to Protect' Children," *The Guardian*, (Aug. 30, 2005), and email release from Yaman Akdeniz to cyber-rights-UK@cyber-right.org listserv (Aug. 31, 2005).

[152] Rotella's site gives the date as Dec. 23 (Wed.), but this appears to be a typo.

[153] The library is in Topton, Pennsylvania and is part of the Berks County library system; email from Pam Rotella to Marjorie Heins (Feb. 20, 2006).

and "K-12 sex education."[154] St. Bernard claims that "each and every website" on the iPrism URL block list has been "reviewed by human eyes, leading to the most accurate database in the industry." Its promotional material elaborates:

> Internet Analysts visit each site and assign it one or more category ratings based on the site's content. This 100% "real person analysis" approach is superior to scanning and rating via software or artificial intelligence technology that use techniques such as keynotes, word pairs or custom dictionaries. These systems are susceptible to a high rate of false positives/negatives. These errors are virtually eliminated with iPrism because the iGuard filter list is a result of careful review by our team of professional analysts.[155]

Nowhere does the promotional literature explain how its staff could possibly analyze the "hundreds of millions" of Web pages that the company states have been reviewed.

To access iPrism's white papers, which explain its technology in more detail, we had to supply contact information on one of the company's Web pages. Within an hour, we were contacted by a sales representative, whom we questioned about the claim of 100% human review. He stuck to this assertion, although acknowledging that it was difficult to believe. He said that the company had classified "several million" Web pages with "maybe a dozen" employees assigned to the task. He acknowledged that "bots" are used to identify potentially questionable content, and that the reviewers probably spend less than ten seconds on average reviewing any given site.[156]

Even if their employees' review took only one second per Web page, iPrism's claims are not credible, given the "several million" pages the salesman said had been reviewed, or the "hundreds of millions" claimed in the company's "iPrism FAQs."[157]

New York Times: SmartFilter Blocks Boing Boing

Tom Zeller, Jr., "Popular Web Site Falls Victim to a Content Filter," *New York Times* (Mar. 6, 2006)

This article reported that SmartFilter, as installed at the offices of Halliburton, Fidelity, and many other major corporations, blocked the popular Web site Boing Boing because, it seemed, "a site reviewer at Secure Computing spotted something fleshy at Boing Boing and tacked the Nudity category onto the blog's classification." Protests from employees, "now deprived of their daily fix of tech-ephemera," led to an inquiry to Secure Computing. Evidently, the offending page discussed two history books about adult magazines from the art publisher Taschen. Secure Computing explained that it would take far too long for its staff to review the tens of thousands of posts on Boing Boing, "so, in order to fulfill their promise to their customers, for Secure Computing, half a percent is the same as 100 percent," and the entire site is blocked.

[154] "iPrism—Site Rating Category Descriptions," www.stbernard.com/products/iprism/products_iprism-cats.asp (visited 2/1/06).

[155] St. Bernard Software, "iPrism FAQs" (Feb. 2003).

[156] John Owens, St. Bernard sales representative, phone conversation with Marjorie Heins (Feb. 1, 2006).

[157] A careful reading of the product literature suggests that the company doesn't claim human review for updates, once a site is on the block list; the FAQ says: "the database is updated on a daily basis via *automatic* incremental updates" (emphasis added).

Conclusions and Recommendations

The more sophisticated and statistically oriented tests of filtering software in the period from 2001-06 differ widely in their purposes and results. Although statistics and percentages in this field of research can be misleading, one conclusion is clear from all of the studies: filters continue to block large amounts of valuable information. Even the expert witnesses for the government in the CIPA case, who attempted to minimize the rates of error, reported substantial overblocking. Internet filters are powerful, often irrational, censorship tools.

Filters force the complex and infinitely variable phenomenon known as human expression into deceptively simple categories. They reduce the value and meaning of expression to isolated words and phrases. An inevitable consequence is that they frustrate and restrict research into health, science, politics, the arts, and many other areas.

Filters are especially dangerous because they block large amounts of expression in advance. This "prior restraint" aspect of filtering contrasts sharply with the American tradition of punishing speech only after it is shown to be harmful. Filters erect barriers and taboos rather than educating youth about media literacy and sexual values. They replace educational judgments by teachers and librarians with censorship decisions by private companies that usually do not disclose their operating methods or their political biases, and that often make misleading, if not false, marketing claims.

CIPA—the law mandating filters in schools and libraries that receive federal aid—is not likely to be repealed very soon, nor are most school districts or libraries likely to throw away filters despite their dangers and flaws. There are, however, many things that can be done to reduce the ill effects of CIPA and promote noncensorious methods of increasing Internet safety. These include:

- Avoiding filters manufactured by companies whose blocking categories reflect a particular ideological viewpoint. These may be appropriate for home or church use, but not for public libraries and schools.
- Choosing filters that easily permit disabling, as well as unblocking of particular wrongly blocked sites.
- Only activating the "sexually explicit" or similar filtering category, since CIPA only requires blocking of obscenity, child pornography, and "harmful to minors" material, all of which must, under the law, contain "prurient" or "lascivious" sexual content.
- Establishing a simple, efficient process for changing incorrect or unnecessary settings.
- Promptly and efficiently disabling filters on request from adults, or, if permitted by the portion of CIPA that applies to them, from minors as well.
- Configuring the default page—what the library user sees when a URL is blocked—to educate the user on how the filter works and how to request disabling.
- Developing educational approaches to online literacy and Internet safety. Despite the superficial appeal of filters, they are not a solution to concerns about pornography or other questionable content online. Internet training, sex education, and media literacy are the best ways to protect the next generation.

Bibliography

American Civil Liberties Union, *Censorship in a Box: Why Blocking Software Is Wrong for Public Libraries* (Sept. 16, 2002), www.aclu.org/Privacy/Privacy.cfm?ID=13624&c=252 (visited 3/29/05).

American Civil Liberties Union, *Fahrenheit 451.2: Is Cyberspace Burning?* (1997), www.aclu.org/privacy/speech/15145pub20020317.html (visited 2/3/06).

American Library Association, "From the Field," www.ala.org/ala/washoff/Woissues/civilliberties/cipaWeb/adviceresources/fromthefield.html (visited 3/22/05).

American Library Association v. United States, 201 F. Supp.2d 401 (E.D. Pa. 2002), reversed, 123 S.Ct. 2297 (2003), Expert reports:

Geoffrey Nunberg, Plaintiffs' Expert Witness Report (undated) and Expert Rebuttal Report (Nov. 30, 2001).

Benjamin Edelman, Plaintiffs' Expert Witness Initial Report (Oct. 15, 2001), Rebuttal Report (Nov. 30, 2001), and Supplemental Report (March 13, 2002), cyber.law.harvard.edu/people/edelman/mul-v-us (visited 3/11/06).

Joseph Janes, Plaintiffs' Expert Witness Report (Oct. 15, 2001).

Anne Lipow, Plaintiffs' Expert Witness Report (Oct. 12, 2001).

Cory Finnell, Defendants' Expert Witness Report (Oct. 15, 2001).

eTesting Labs. *Updated Web Content Filtering Software Comparison,* Report prepared under contract from the U.S. Department of Justice (Oct. 2001)

Joseph Anderson, "CIPA and San Francisco, California: Why We Don't Filter," *WebJunction* (Aug. 31, 2003), www.webjunction.org/do/DisplayContent?id=996 (visited 7/22/05).

Joseph Anderson, "CIPA Reports From the Field," *WebJunction* (Aug. 31, 2003), www.webjunction.org/do/DisplayContent?id=995 (visited 1/31/06).

Associated Press, "Libraries Oppose Internet Filters, Turn Down Federal Funds" (June 13, 2004), www.boston.com/dailynews/165/region/Libraries_oppose-Internet_filt:.shtml (visited 6/16/04).

Lori Bowen Ayre, *Filtering and Filter Software* (American Library Association Library Technology Reports, 2004).

Carson Block, *A Comparison of Some Free Internet Content Filters and Filtering Methods* (Colorado State Library, Jan. 2004).

Lisa Bowman, "Filtering Programs Block Candidate Sites," *ZDNet News*, Nov. 8, 2000, news.zdnet.com/2100-9595_22-525405.html (visited 2/3/06).

Alan Brown, "Winners of the Foil the Filter Contest" (Digital Freedom Network, Sept. 28, 2000), users.du.se/~jsv/DFN%20Winners%20of%20Foil%20the%20Filters%20Contest.htm (visited 3/9/06).

Stéphan Brunessaux, *Report on Currently Available COTS Filtering Tools, D5.1, Version 1.0* (MATRA Systèmes & Information, June 28, 2002), www.net-protect.org/en/MSI-WP5-D5.1-v1.0.pdf (visited 2/14/06).

Sylvie Brunessaux *et al.*, *Report on Currently Available COTS Filtering Tools, D2.2, Version 1.0* .(MATRA Systèmes & Information, Oct. 1, 2001), np1.net-protect.org/en/MSI-WP2-D2.2-v1.0.pdf (visited 2/28/06).

David Burt, "ALA Touts Filter Study Whose Own Author Calls Flawed" (Filtering Facts press release, Feb. 18, 2000).

David Burt, "Study of Utah School Filtering Finds 'About 1 in a Million' Web Sites Wrongly Blocked" (Filtering Facts, Apr. 4, 1999), www.sethf.com/anticensorware/history/smartfilter-david-burt.php (visited 2/3/06).

Valerie Byrd, Jessica Felker, & Allison Duncan, "BESS Won't Go There: A Research Report on Filtering Software," 25:½ *Current Studies in Librarianship* (2001), 7-19.

Censorware Project, *Blacklisted by Cyber Patrol: From Ada to Yoyo* (Dec. 22, 1997), censorware.net/reports/cyberpatrol/ada-yoyo.html (visited 2/10/06) .

Censorware Project, *Blacklisted By Cyber Patrol: From Ada to Yoyo – The Aftermath* (Dec. 25, 1997), censorware.net/reports/cyberpatrol/aftermath.html (visited 2/10/06).

Censorware Project, "Cyber Patrol and Deja News" (Feb. 17, 1998), censorware.net/reports/dejanews/index.html (visited 2/10/06).

Censorware Project, *Passing Porn, Banning the Bible: N2H2's Bess in Public Schools* (2000), censorware.net/reports/Bess/index.html (visited 2/9/06).

Censorware Project, *Protecting Judges Against Liza Minnelli: The WebSENSE Censorware at Work* (June 21, 1998), censorware.net/reports/liza.html (visited 2/9/06).

Censorware Project, *The X-Stop Files: Déjà Voodoo* (1999), censorware.net/reports/xstop/index.html (visited 2/10/06).

Center for Media Education, *Youth Access to Alcohol and Tobacco Web Marketing: The Filtering and Rating Debate* (Oct. 1999).

Mary Chelton, "Re: Internet Names and Filtering Software," in American Library Association Office for Intellectual Freedom newsgroup: *ala1.ala.org* (Mar. 5, 1997), www.peacefire.org/archives/surfwatch.archie-r-dykes-hospital.txt (visited 2/14/06).

Commission on Child Online Protection ("COPA" Commission), *Report to Congress* (Oct. 20, 2000), www.copacommission.org/report/ (visited 8/29/02).

Computing Which? press release, "Software Alone Can't Create a Safe Online Playground" (Aug. 30, 2005), www.which.net/press/releases/computing/050830_safe-online_nr.html (visited 2/23/06).

Consortium for School Networking, *Safeguarding the Wired Schoolhouse: A Briefing Paper on School District Options for Providing Access to Appropriate Internet Content* (June 2001), www.safewiredschools.org/pubs_and_tools/white_paper.pdf (visited 2/3/06)

Walt Crawford, "The Censorware Chronicles," *Cites & Insights* (Mar. 2004), 10, cites.boisestate.edu/civ4i4.pdf (visited 2/23/06).

Drew Cullen, "Cyber Patrol unblocks *The Register,*" *The Register* (Mar. 9, 2001), www.theregister.co.uk/content/6/17465.html (visited 2/3/06).

"Digital Chaperones for Kids," *Consumer Reports* (Mar. 2001), 20–25.

Benjamin Edelman, "Empirical Analysis of Google SafeSearch" (Berkman Center for Internet & Society, Apr. 2003), cyber.law.harvard.edu/people/edelman/google-safesearch/ (visited 2/3/06).

Benjamin Edelman, "Web Sites Sharing IP Addresses: Prevalence and Significance" (Berkman Center for Internet & Society, Feb. 2003), cyber.law.harvard.edu/people/edelman/ip-sharing/ (visited 2/17/06).

Electronic Frontier Foundation/Online Policy Group, *Internet Blocking in Public Schools: A Study on Internet Access in Educational Institutions, Version 1.1* (June 26, 2003), www.eff.org/Censorship/Censorware/net_block_report/net_block_report.pdf (visited 4/26/05).

Electronic Privacy Information Center, *Filters and Freedom 2.0.* (2d ed. David Sobel, ed.) (EPIC, 2001).

Ethical Spectacle press release, "CYBERsitter Blocks *The Ethical Spectacle*" (Jan. 19, 1997), www.spectacle.org/alert/cs.html (visited 2/3/06).

"Filtering Software: Better, But Still Fallible," *Consumer Reports* (June 2005), www.consumerreports.org/cro/electronics-computers/internet-filtering-software-605/overview.htm (visited 2/3/06).

"Filtering Utilities," *PC Magazine* (Apr. 18, 1997).

Seth Finkelstein, "BESS vs. Image Search Engines" (Mar. 2002), sethf.com/anticensorware/Bess/image.php (visited 2/16/06).

Seth Finkelstein, "BESS's Secret Loophole" (Aug. 2001; revised and updated, Nov. 2002), sethf.com/anticensorware/bess/loophole.php (visited 2/16/06)

Seth Finkelstein, "SmartFilter's Greatest Evils" (Nov. 16, 2000), sethf.com/anticensorware/smartfilter/greatestevils.php (visited 2/3/06).

Seth Finkelstein, "SmartFilter – I've Got a Little List" (Dec. 7, 2000), sethf.com/anticensorware/smartfilter/gotalist.php (visited 2/3/06).

Free Expression Policy Project, *Fact Sheet on Internet Filters* (n.d.), www.fepproject.org/factsheets/filtering.html (visited 1/31/06).

Free Expression Policy Project, *Fact Sheet on Sex and Censorship* (n.d.), www.fepproject.org/factsheets/sexandcensorship.html (visited 2/10/06).

Gay & Lesbian Alliance Against Defamation, *Access Denied: The Impact of Internet Filtering Software on the Lesbian and Gay Community* (Dec. 1997), www.glaad.org/documents/media/AccessDenied1.pdf (visited 2/3/06).

Gay & Lesbian Alliance Against Defamation, *Access Denied, Version 2.0: The Continuing Threat Against Internet Access and Privacy and its Impact on the Lesbian, Gay, Bisexual and Transgender Community* (1999), www.glaad.org/documents/media/AccessDenied2.pdf (visited 2/3/06).

Gay & Lesbian Alliance Against Defamation press release, "Gay Sites Netted in Cyber Patrol Sting" (Dec. 19, 1997), www.glaad.org/action/al_archive_detail.php?id=1932& (visited 2/3/06).

Gay & Lesbian Alliance Against Defamation, press release, "We-Blocker.com: Censoring Gay Sites was 'Simply a Mistake'" (Aug. 5, 1999), www.glaad.org/action/al_archive_detail.php?id=1511& (visited 2/9/06).

Paul Greenfield, Peter Rickwood, & Huu Cuong Tran, *Effectiveness of Internet Filtering Software Products* (CSIRO Mathematical and Information Sciences, 2001), www.aba.gov.au/newspubs/documents/filtereffectiveness.pdf (visited 2/14/06).

Ann Grimes *et al.*, "Digits: Expletive Deleted," *Wall Street Journal* (May 6, 1999), B4.

A. Gulli & A. Signorini, "The Indexable Web is More Than 11.5 Billion Pages," *WWW 2005* (May 10–14, 2005), www.cs.uiowa.edu/~asignori/web-size/size-indexable-web.pdf (visited 3/3/06).

Katie Hafner, "Library Grapples with Internet Freedom," *New York Times* (Oct. 15, 1998), G1.

Derek Hansen, *CIPA: Which Filtering Software to Use?* (WebJunction, Aug. 31, 2003), www.Webjunction.org/do/DisplayContent?id=1220 (visited 2/9/06).

Anemona Hartocollis, "Board Blocks Student Access to Web sites: Computer Filter Hobbles Internet Research Work," *New York Times* (Nov. 10, 1999), B1.

Bennett Haselton, "Amnesty Intercepted: Global Human Rights Groups Blocked by Web Censoring Software" (Peacefire, Dec. 12, 2000), www.peacefire.org/amnesty-intercepted (visited 2/9/06).

Bennett Haselton, "AOL Parental Controls Error Rate for the First 1,000 .com Domains" (Peacefire, Oct. 23, 2000), www.peacefire.org/censorware/AOL/first-1000-com-domains.html (visited 2/9/06).

Bennett Haselton, "BabelFish Blocked By Censorware" (Peacefire, Feb. 27, 2001), www.peacefire.org/babelfish (visited 2/9/06).

Bennett Haselton, "BESS Error Rate for 1,000 .com Domains" (Peacefire, Oct. 23, 2000), www.peacefire.org/censorware/BESS/second-1000-com-domains.html (visited 2/9/06).

Bennett Haselton, "Blocking Software FAQ" (Peacefire, n.d.), www.peacefire.org/info/blocking-software-faq.html (visited 2/10/06).

Bennett Haselton, "Columnist Opines Against Censorware, Gets Column Blocked" (Censorware Project, Mar. 29, 2001), censorware.net/article.pl?sid=01/03/29/1730201&mode=nested&threshold= (visited 2/9/06).

Bennett Haselton, "Cyber Patrol Error Rate for First 1,000 .com Domains" (Peacefire, Oct. 23, 2000), www.peacefire.org/censorware/Cyber_Patrol/first-1000-com-domains.html (visited 1/31/06).

Bennett Haselton, "CYBERsitter: Where Do We Not Want You to Go Today?" (Peacefire, Nov. 5-Dec. 11, 1996), www.spectacle.org/alert/peace.html (visited 2/9/06).

Bennett Haselton, "SafeServer Error Rate for First 1,000 .com Domains" (Peacefire, Oct. 23, 2000), www.peacefire.org/censorware/FoolProof/first-1000-com-domains.html (visited 2/9/06).

Bennett Haselton, "Sites Blocked By Cyber Sentinel" (Peacefire, Aug. 2, 2000), www.peacefire.org/censorware/Cyber_Sentinel/cyber-sentinel-blocked.html (visited 2/9/06).

Bennett Haselton, "Sites Blocked By FamilyClick" (Peacefire, Aug. 1, 2000), www.peacefire.org/censorware/FamilyClick/familyclick-blocked.html (visited 2/9/06).

Bennett Haselton, "Study of Average Error Rates for Censorware Programs" (Peacefire, Oct. 23, 2000), www.peacefire.org/error-rates (visited 2/9/06).

Bennett Haselton, "SurfWatch Error Rates for First 1,000 .com Domains" (Peacefire, Aug. 2, 2000), www.peacefire.org/censorware/SurfWatch/first-1000-com-domains.html (visited 2/9/06).

Bennett Haselton, "Teen Health Sites Praised in Article, Blocked by Censorware" (Peacefire, Mar. 23, 2001), www.peacefire.org/censorware/teen-health-sites-blocked.shtml (visited 2/9/06).

Bennett Haselton & Jamie McCarthy, "Blind Ballots: Web Sites of U.S. Political Candidates Censored by Censorware" (Peacefire, Nov. 7, 2000), www.peacefire.org/blind-ballots (visited 2/9/06).

Marjorie Heins, "Internet Filters Are Now a Fact of Life, But Some Are Worse Than Others" (Free Expression Policy Project, Sept. 2, 2004), www.fepproject.org/reviews/ayre.html (visited 3/29/05) (review of Lori Bowen Ayre, *Filtering and Filter Software*).

Christopher Hunter, *Filtering the Future?: Software Filters, Porn, PICS, and the Internet Content Conundrum* (Master's thesis, Annenberg School for Communication, University of Pennsylvania, July 1999), www.copacommission.org/papers/hunter-thesis.pdf (visited 2/9/06).

"Internet Filter Software Blocks Only Pro-Gun Sites," *American Rifleman* (Nov. 2003).

Paul Jaeger, John Carlo Bertot, & Charles McClure, "The Effects of the Children's Internet Protection Act (CIPA) in Public Libraries and its Implications for Research: A Statistical, Policy, and Legal Analysis," 55(13) *Journal of the American Society for Information Science and Technology* 1131 (2004), www3.interscience.wiley.com/cgi-bin/fulltext/109089142/PDFSTART (visited 3/14/06).

Paul Jaeger & Charles McClure, "Potential Legal Challenges to the Application of the Children's Internet Protection Act in Public Libraries," *First Monday* (Jan. 16, 2004), www.firstmonday.org/issues/issue9_2/jaeger/index.html (visited 3/22/05).

Eddy Jansson & Matthew Skala, *The Breaking of Cyber Patrol®4* (Mar. 11, 2000), pratyeka.org/library/text/jansson%20and%20skala%20-%20the%20breaking%20of%20cyberpatrol%204.txt (visited 1/31/06).

L. Kelly, "Adam and Eve Get Caught in 'Net Filter," *Wichita Eagle* (Feb. 5, 1998), 13A.

Marie-José Klaver, "What Does CYBERsitter Block?" (updated June 23, 1998), www.xs4all.nl/~mjk/CYBERsitter.html (visited 2/9/06).

Lars Kongshem, "Censorware – How Well Does Internet Filtering Software Protect Students?" *Electronic School* (Jan. 1998), www.electronic-school.com/0198f1.html (visited 2/1/06).

Christopher Kryzan, "Re: SurfWatch Censorship Against Lesbigay WWW Pages" (email release, June 14, 1995), www.cni.org/Hforums/roundtable/1995-02/0213.html (visited 2/14/06).

Wendy Leibowitz, "Shield Judges from Sex?" *National Law Journal* (May 18, 1998), A7.

Amanda Lenhart, *Protecting Our Teens Online* (PEW Internet & American Life Project, Mar. 17, 2005), www.pewinternet.org/pdfs/PIP_Filters_Report.pdf (visited 2/10/06).

Lawrence Lessig, "What Things Regulate Speech: CDA 2.0 vs. Filtering." 38 *Jurimetrics* 629 (1998), cyber.law.harvard.edu/works/lessig/what_things.pdf (visited 2/9/06).

Douglas Levin & Sousan Arafeh, *The Digital Disconnect: The Widening Gap Between Internet-Savvy Students and Their Schools* (American Institutes for Research/Pew Internet and American Life Project, Aug. 14, 2002), www.pewinternet.org/report_display.asp?r=67 (visited 2/9/06).

John Leyden, "Porn-filter Disabler Unleashed," *The Register* (Dec. 19, 2000), www.theregister.co.uk/content/archive/15578.html (visited 2/9/06).

Greg Lindsay, "CYBERsitter Decides To Take a Time Out," *Time Digital*, Aug. 8, 1997), available at the Internet Archive Wayback Machine, Web.archive.org/Web/20000830022313/www.time.com/time/digital/daily/0,2822,12392,00.html (visited 2/16/06).

Robert Lipschutz, "Web Content Filtering: Don't Go There," *PC Magazine* (Mar. 16, 2004), www.pcmag.com/article2/0,1759,1538518,00.asp (visited 6/1/04).

Brian Livingston, "AOL's 'Youth Filters' Protect Kids From Democrats," *CNet News* (Apr. 24, 2000), news.com.com/2010-1071-281304.html (visited 2/9/06).

Mainstream Loudoun, et al. v. Board of Trustees of the Loudoun County Library, 24 F. Supp.2d 552 (E.D. Va. 1998), Case Documents:

Plaintiffs' Complaint for Declaratory and Injunctive Relief (Dec. 22, 1997).

"Internet Sites Blocked by X-Stop," Plaintiffs' Exhibit 22 (Oct. 1997).

ACLU Memoranda (Jan. 27-Feb. 2, 1998).

Plaintiffs-Intervenors' Complaint for Declaratory and Injunctive Relief (Feb. 5, 1998).

ACLU Memoranda (June 17-23, 1998).

Karen Schneider, Plaintiffs' Expert Witness Report (June 18, 1998).

David Burt, Defendants' Expert Witness Report (July 14, 1998).

Michael Welles, Plaintiffs' Expert Witness Report (Sept. 1, 1998).

Loren Kropat, Second Declaration (Sept. 2, 1998).

Jamie McCarthy, "Lies, Damn Lies, and Statistics" (Censorware Project, June 23, 1999, updated Sept. 7, 2000), censorware.net/reports/utah/followup/index.html (visited 1/31/06).

Jamie McCarthy, "Mandated Mediocrity: Blocking Software Gets a Failing Grade" (Peacefire/Electronic Privacy Information Center, Oct. 2000), www.peacefire.org/censorware/BESS/MM (visited 1/31/06).

Kieren McCarthy, "Cyber Patrol Bans *The Register*," *The Register* (Mar. 5, 2001), www.theregister.com/content/6/17351.html (visited 2/9/06).

Declan McCullough, "U.S. Blunders with Keyword Blacklist," *C/net news* (May 3, 2004), news.com.com/2010-1028-5204405.html?tag=nefd.acpro (visited 3/29/05).

Brock Meeks & Declan McCullagh, "Jacking in From the 'Keys to the Kingdom' Port," *CyberWire Dispatch* (July 3, 1996), cyberwerks.com/cyberwire/cwd/cwd.96.07.03.html (visited 1/31/06).

Walter Minkel, "A Filter That Lets Good Information In," *TechKnowledge* (Mar. 1, 2004), www.schoollibraryjournal.com/article/CA386721?display=TechKnowledgeNews&industryi=TechKnowledge&industryid=1997&verticalid=152& (visited 2/9/06).

Mary Minow, "Lawfully Surfing the Net: Disabling Public Library Internet Filters to Avoid More Lawsuits in the United States," *First Monday,* (Apr. 2004), firstmonday.org/issues/issue9_4/minow/ (visited 2/9/06).

Bonnie Rothman Morris, "Teenagers Find Health Answers with a Click," *New York Times* (Mar. 20, 2001), F8.

Kathryn Munro, "Filtering Utilities," *PC Magazine* (Apr. 8, 1997), 235-40.

Corey Murray, "Overzealous Filters Hinder Research," *eSchool News Online* (Oct. 13, 2005), www.eschoolnew.com/news/showStoryts.cfm?ArticleID=5911 (visited 10/20/05).

Ann Myrick, *Reader's Block: Internet Censorship in Rhode Island Public Libraries* (Rhode Island American Civil Liberties Union, Apr. 2005), www.riaclu.org/friendly/documents/2005libraryinternetreport.pdf (visited 2/24/06).

N2H2 press release, "N2H2 Launches Online Curriculum Partners Program, Offers Leading Education Publishers Access to Massive User Base" (Sept. 6, 2000).

National Research Counsel, *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert Lin, eds.) (2002), newton.nap.edu/books/0309082749/html/R1.html (visited 2/9/06).

Chris Oakes, "Censorware Exposed Again," *Wired News* (Mar. 9, 2000), www.wired.com/news/technology/0,1282,34842-2,00.html (visited 2/9/06).

Online Policy Group, "Online Oddities and Atrocities Museum" (n.d.), www.onlinepolicy.org/research/museum.shtml (visited 2/9/06).

OpenNet Initiative, *A Starting Point: Legal Implications of Internet Filtering* (Sept. 2004), opennetinitiative.net/docs/Legal_Implications.pdf (visited 2/9/06).

OpenNet Initiative, *Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran* (May 3, 2004), www.opennetinitiative.net/advisories/001/ (visited 2/9/06).

OpenNet Initiative, "Filtering Technologies Database" (2004), www.opennetinitiative.net/modules.php?op=modload&name=FilteringTech&file=index (visited 2/23/06).

OpenNet Initiative, "Introduction to Internet Filtering" (2004), www.opennetinitiative.net/modules.php?op=modload&name=Archive&file=index&req=viewarticle&artid=5 (visited 1/31/06).

Clarence Page, "Web Filters Backfire on their Fans," *Chicago Tribune*, Mar. 28, 2001, 19.

Peacefire, "Analysis of First 50 URLs Blocked by I-Gear in the .edu Domain" (Mar. 2000), www.peacefire.org/censorware/I-Gear/igear-blocked-edu.html (visited 2/9/06).

Peacefire, "Analysis of First 50 URLs Blocked by X-Stop in the .edu Domain" (Jan. 2000), www.peacefire.org/censorware/X-Stop/xstop-blocked-edu.html (visited 2/9/06).

Peacefire, "'BESS, the Internet Retriever' Examined" (2000), www.peacefire.org/censorware/BESS (visited 2/9/06).

Peacefire, "CYBERsitter Examined" (2000), www.peacefire.org/censorware/CYBERsitter (visited 3/10/06).

Peacefire, "I-Gear Examined" (2000), www.peacefire.org/censorware/I-Gear (visited 2/9/06).

Peacefire, "Inaccuracies in the 'CyberNOT Search Engine,'" (n.d.), www.peacefire.org/censorware/Cyber_Patrol/cybernot-search-engine.html (visited 3/9/06).

Peacefire, "More Sites Found Blocked by Cyber Patrol" (Jan. 2002), www.peacefire.org/censorware/Cyber_Patrol/jan-2002-blocks.shtml (visited 1/31/06).

Peacefire, "Net Nanny Examined" (2000), www.peacefire.org/censorware/Net_Nanny (visited 2/9/06).

Peacefire, "SafeSurf Examined" (2000), www.peacefire.org/censorware/SafeSurf (visited 2/9/06).

Peacefire, "Sites Blocked by ClickSafe" (July 2000), www.peacefire.org/censorware/ClickSafe/screenshots-copacommission.html (visited 2/9/06).

Peacefire, "SmartFilter Examined" (1997), www.peacefire.org/censorware/SmartFilter (visited 2/9/06).

Peacefire, "SurfWatch Examined" (2000), www.peacefire.org/censorware/SurfWatch (visited 2/9/06).

Peacefire, "WebSENSE Examined" (2002), www.peacefire.org/censorware/WebSENSE/ (visited 1/31/06).

Peacefire, "X-Stop Examined" (1997–2000), www.peacefire.org/censorware/X-Stop (visited 2/9/06).

Paul Resnick, Derek Hansen, & Caroline Richardson, "Calculating Error Rates for Filtering Software," 47:9 *Communications of the ACM* 67-71 (Sept. 2004).

Caroline Richardson *et al.,* "Does Pornography-Blocking Software Block Access to Health Information on the Internet?" 288:22 *Journal of the American Medical Association* 2887-94 (Dec. 11, 2002).

Matt Richtel, "Tables Turn on a Filtering Site as It Is Temporarily Blocked," *New York Times* (Mar. 11, 1999), G3.

Victoria Rideout, Caroline Richardson, & Paul Resnick, *See No Evil: How Internet Filters Affect the Search for Online Health Information* (Kaiser Family Foundation, Dec. 2002), www.kff.org/entmedia/20021210a-index.cfm (visited 2/17/06)

Pam Rotella, "Internet 'Protection' (CIPA) Filtering Out Political Criticism," Blog post, PamRotella.com (Nov. 22, 2005; updated Nov. 23, 2005), www.pamrotella.com/polhist/rants/rants001/rants00019.html (visited 11/23/05).

Ana Luisa Rotta, *Report on Filtering Techniques and Approaches*, *D2.3, Version 1.0* (MATRA Systèmes & Information, Oct. 23, 2001), np1.net-protect.org/en/OPT-WP2-D2.3-v1.0.pdf (visited 2/28/06).

Karen Schneider, *A Practical Guide to Internet Filters* (Neal-Schulman Publishers, 1997).

Secure Computing press release, "Censorware Project Unequivocally Confirms Accuracy of SmartFilter in State of Utah Education Network" (June 18, 1999), www.securecomputing.com/archive/press/1999/sfcensorware-49.html (visited 2/3/06).

Secure Computing, "Education and the Internet: A Balanced Approach of Awareness, Policy and Security" (1999), www.securecomputing.com/index.cfm?skey=227 (visited 2/3/06).

Michael Sims *et al.*, *Censored Internet Access in Utah Public Schools and Libraries* (Censorware Project, Mar. 1999), censorware.net/reports/utah/utahrep.pdf (visited 1/31/06).

Electronic Privacy Information Center, "Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet" (1997), www.epic.org/reports/filter_report.html (visited 3/10/06).

SurfControl press release, "Cyber Patrol Tells COPA Commission that Market for Internet Filtering Software to Protect Kids is Booming" (July 20, 2000).

Lynn Sorenson Sutton, *Experiences of High School Students Conducting Term Paper Research Using Filtered Internet Access* (PhD dissertation, the Graduate School of Wayne State University, 2005).

Michael Swaine, "WebSENSE Blocking Makes No Sense," *WebReview.com* (June 4, 1999), www.ddj.com/documents/s=2366/nam1011136473/index.html (visited 2/9/06).

Jim Tyre, "Sex, Lies and Censorware" (Censorware Project, May 14, 1999), censorware.net/article.pl?sid=01/03/05/0622253 (visited 2/9/06).

U.S. Department of Commerce, National Telecommunications and Information Administration, *Report to Congress: Children's Internet Protection Act: Study of Technology Protection Measures in Section 1703* (Aug. 15, 2003), www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/CIPAreport_08142003.htm (visited 3/29/05).

Jonathan Wallace, "Cyber Patrol: The Friendly Censor" (Censorware Project, Nov. 22, 1997), censorware.net/essays/cypa_jw.html (visited 2/9/06).

Jonathan Wallace, "The X-Stop Files" (Censorware Project, Oct. 5, 1997), censorware.net/essays/xstop_files_jw.html (visited 2/9/06).

"White House Accidentally Blocked by SurfWatch," 2:5 *Netsurfer Digest* (Feb. 19, 1996), www.ecst.csuchico.edu/~zazhan/surf/surf2_5.html#BS6 (visited 2/14/06).

Nancy Willard, *Filtering Software: The Religious Connection* (Responsible Netizen, 2002), responsiblenetizen.org/onlinedocs/documents/religious1.html (visited 2/9/06).

Tom Zeller, Jr., "Popular Web Site Falls Victim to a Content Filter," *New York Times* (Mar. 6, 2006), C3.

BRENNAN CENTER FOR JUSTICE
at NYU SCHOOL OF LAW
Free Expression Policy Project
161 Avenue of the Americas, 12th floor
New York, NY 10013
212-998-6730
www.brennancenter.org
www.fepproject.org

FEPP's Previous Policy Reports are all available at **www.fepproject.org:**

- *Media Literacy: An Alternative to Censorship* (2002)
- *"The Progress of Science and Useful Arts": Why Copyright Today Threatens Intellectual Freedom* (2003)
- *Free Expression in Arts Funding* (2003)
- *The Information Commons* (2004)
- *Will Fair Use Survive? Free Expression in the Age of Copyright Control* (2005)