# UNITED STATES COPYRIGHT OFFICE

# Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works

## Docket No. RM 2002-4

## JOINT REPLY COMMENTS

of

N2H2, INC.,
8e6 Technologies,
Bsafe Online,

Submitted by:
David Burt
N2H2, Inc.
900 4th Avenue, Suite 3600
Seattle, WA 98164
Tel: (206) 982-1130; Fax: (509) 271-4226
Email: dburt@n2h2.com

February 18, 2003

**Class of works:** Compilations consisting of lists of websites blocked by filtering software applications.

**Summaries of the arguments to which we are replying:**

Comment #33, Arnold P. Lutzker on behalf of Library Associations:
"Absent evidence that the problems which originally warranted the exemptions have been corrected by the marketplace, the exemption issued in 2000 for “literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage, or obsoleteness” and the exemption for “compilations consisting of lists of websites blocked by filtering software applications" should be extended into the three-year period from October 28, 2003 to October 28, 2006."

Comment #29, Shawn Hernan, on behalf of the CERT Coordination Center
"Compilations consisting of lists of websites blocked by filtering software applications -- The proposed exemption is fully supported by the rationale adopted by the Register in the initial exemption rulemaking under Section 1201(1)(a)(3). There have been no changes in the marketplace or in the related technologies or business practices that mitigate against the necessity for continuing the exemption."

Comment #32,  Samuel Greenfeld
"Previously, the Librarian of Congress decided to exempt this class of works from the access provisions of the Digital Millennium Copyright Act (DMCA). Research done under this exemption has resulted in a number of findings, many of which are of interest to the general public. It is therefore requested that this class be considered for renewal."

Comment #31, Seth Finkelstein
"Discovering what is truly banned by censorware has been a matter of public debate. Such evidence has played an important role in litigation such as the _Mainstream Loudoun v. Loudoun County Library_ library censorware case, or the Children's Internet Protection Act (CIPA) case. Studies of censorware blacklists are vastly hindered by not being able to access those blacklists. In particular, studying structural, architectural issues, such as "loophole" sites, requires access to the decrypted blacklist."

**About the Joint Commenters**
The undersigned organizations appreciate the opportunity to respond to the Notice of Inquiry issued by the Copyright Office and published in the Federal Register on October 5, 2002. See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Fed. Reg. Volume 67, Number 199, Page 63578-63582 (2002). We also respond here to certain comments received in the first round of this proceeding.

The companies submitting joint comments all manufacture Internet filtering software. Simply defined, Internet filtering software is software that is designed to enable organizations or individuals to block access to specific types of web content, which may be deemed inappropriate for a user or group of users.

**About N2H2**
N2H2, Inc. is a global Internet content filtering company whose software helps customers control, manage and understand their Internet use by filtering content, monitoring access and delivering concise user activity reports. N2H2's Bess and Sentian product lines are used by millions in businesses, schools, and libraries around the world.

**About 8e6 Technologies**
8e6 Technologies is a privately held software and hardware developer, specializing in Internet Filtering and Reporting (IFR) solutions for thousands of businesses, ISPs and schools throughout the world. Located in Orange, California, 8e6 assists clients in managing the impact of the Internet on employee productivity, legal liability and network resources, through flexible, accurate and high speed filtering of Internet content.

**About Bsafe Online**
Bsafe Online is a privately held Application Service Provider (ASP) incorporated in January of 2001. Bsafe's primary mission is providing advanced Internet protective services to families, small schools and SOHO environments through its strategic partners. Services include content filtering, accountability reporting and protected email technology.

## Introduction

On October 28, 2000, the Library of Congress created an exemption from liability under 17 U.S.C. § 1201(a)(1)(A), the Digital Millennium Copyright Act (DMCA) for circumvention in order to gain access to “compilations consisting of lists of websites blocked by filtering software applications.”[1] The Library of Congress implemented this exemption at the recommendation of the copyright office on the basis of several commenters, which found that:

> *…a persuasive case was made that the existence of access control measures has had an adverse effect on criticism and comment, and most likely news reporting, and that the prohibition on circumvention of access control measures will have an adverse effect.*[2]

The Copyright Office stated several arguments that might have been made on behalf of filtering software companies, but noted that "no commenters or witnesses came forward to make such an assertion,"[3] and accepted the facts asserted by the commenters favoring the exemption because "no one else on the record has asserted otherwise."[4]

Notably, none of the companies which manufacture filtering software submitted comments during the 2000 rule making process. The reason for this is very simple: the filtering software companies were unaware of the proceedings, and had no idea that important copyright protections extended to other software companies were in jeopardy for filtering software.

It is unfortunate that the Copyright Office was not presented with all the facts regarding the accessibility of Internet filtering software databases. A number of the comments submitted in favor of the filtering software exemption contained serious inaccuracies and misrepresentations of filtering software databases that went unrefuted.

As the Copyright Office is now reconsidering the exemption for filtering software databases, the filtering software industry is pleased to offer a response to those commenters who are seeking a renewal of the filtering software exemption.

The widespread availablitlity of filtering software today imparts considerable public benefits, not just in the United States but around the world. Most importantly, filtering software protects millions of children from the damaging and salacious content available on the Internet. Additionally, filtering helps companies and government agencies to protect their employees from liability, as well as conserve valuable bandwidth and enhance productivity.

The circumvention of copyright protection for filtering software databases conveys no such discernable public benefits. Rather, such circumventions have in the past, and will in the future, cause harm to the filtering industry, and the ability of parents, schools, and libraries to protect children.

For these reasons, the request for exemption should be denied.

**Summary of Argument in Opposition to the Proposed Exemption**

This comment will demonstrate that circumvention of filtering software should not be permitted because it will adversely affect the filtering industry that is essential for the growth and promotion of the Internet. If filtering companies cannot control access to their databases, it will be difficult for filtering companies to profit from their databases. Fewer filtering databases will be available for use, and parents will be robbed of vital tools for protecting their children.

Moreover, circumvention is not necessary for any reasoned analysis of filtering software because of existing methods that do not involve circumvention. Courts have drawn conclusions of fact and of law related to filters, government commissions have evaluated filters and issued findings, and journalists have investigated filters without research derived from the circumvention of copyright protection measures. In contrast, research derived from the decryption of filtering software has played no meaningful role in court cases, journalism, legislation, independent laboratory research, or other examinations by government bodies.

Thus, commenters will demonstrate that exempting filtering software from the prohibition on circumvention of technological measures would damage both the public and the filtering industry with no corresponding benefit to any element of society.

## About Filtering Databases

Simply defined, Internet filtering software is software that is designed to enable organizations or individuals to block access to specific types of web content, which may be deemed inappropriate for a user or group of users.

There are multiple ways to accomplish content filtering, such as blocking web pages based on the appearance of certain words and phrases, or allowing access only to a "white list" of approved sites.  Of interest to the Copyright Office are those filtering products that use databases of URLs.

A filtering database, in its most simple form, consists of a file of records.  Each record or entry in the database contains two fields or elements: a field containing a Uniform Resource Locator (URL) of a web page or an Internet Protocol (IP) address and a field containing one or more subject categorizations. Below are some sample entries from a filtering database:

| **URL Field** | **Category Field** |
|---|---|
| www.playboy.com | Nudity, Pornography |
| 209.247.228.201 | Nudity, Pornography |
| news.yahoo.com | News |
| sports.yahoo.com | Sports |

In testimony given before the U.S. Congress, Chris Ophus, president of the filtering company FamilyConnect, described how filtering databases are created:

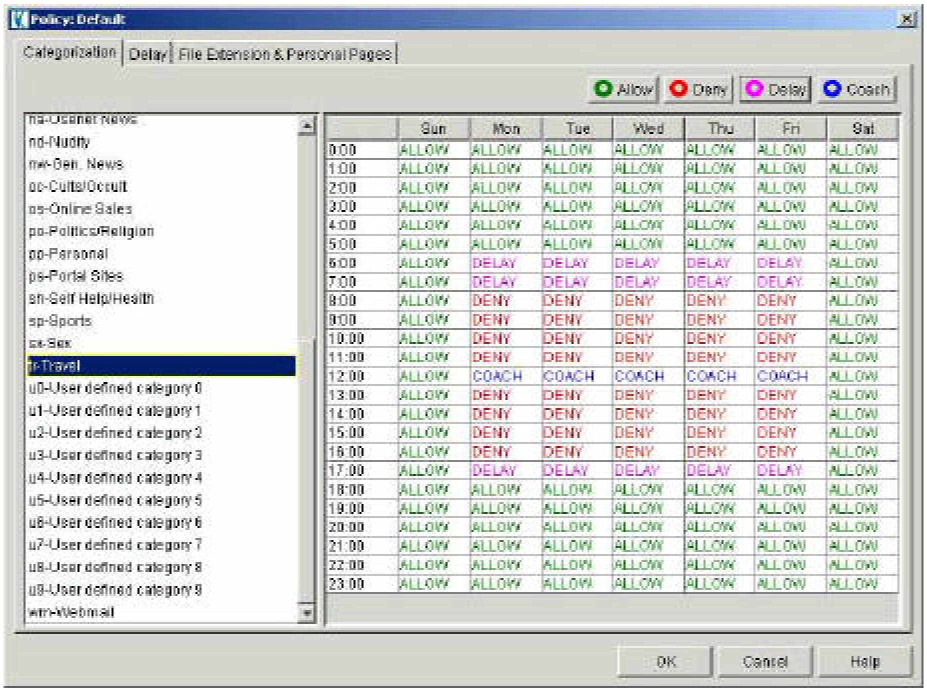
> *URL Filtering*
>
> *This is the most common, and most effective form of filtering, and involves the filtering of a site based on its URL (i.e. its address). It provides more fine-grained control than packet filtering, since a URL can specify a particular page within a large site, rather than specifying the IP address of the computer that hosts the Content.*
>
> *S4F Technologies adds an average of 5,000 – 7,000 new URL's to its database each week. Computer spiders scour the Internet using a sophisticated search mechanism that collects potential sites for human review.  Spidering computers run programs that systematically read through the World Wide Web and collect URL's (Uniform Resource Locators) that match a particular set of criteria established [by] a filtering department.  These computer [programs] can run 24 hours a day and collect potential candidates to be added to the database.  However, spiders are not perfect, and using spiders alone as the mechanism for fortifying a blocked site database would result in overblocking.  That is why human review must be used when accurately building a blocked database.*
>
> *During the human review process, using custom browsers, sites can be positively identified and properly added to the database.  As soon as a site is added, it is active in the blocked list for all to use.  If a site is inadvertently blocked, it is reviewed and a decision is made within 24 at the most.  If the site contains Child Pornography it is automatically forwarded to the National Center for Missing and Exploited Children.*

> *One of the challenges facing filtering departments is managing the constant change of the Internet. When a website is reviewed, it may not contain obscene material, but at some later point, the author of the website may change the content that now would be considered inappropriate. Conversely, a site with content that may have at one time been considered pornographic or illegal could change and be perfectly acceptable. So, in addition to keeping up new sites that come online daily, filtering departments must constantly review those sites that are already categorized. Considering the ongoing task of Internet content data management, coupled with the constant change in the Internet snapshot, filtering companies do an amazing job of keeping up.*[5]

Filtering companies do not attempt to hide the structure of their databases, or the criteria they use to create them. Rather, filtering companies usually consider the structure of their databases to be an important marketing tool. 8e6 Technologies provides a 4-page document describing the company's 38-category database.[6] FamilyConnect contains a 2-page document describing the company's 15-category database.[7] N2H2 provides a 7-page document describing the company's 42-category database. [8] Secure Computing provides a 9-page document describing the company's 30-category database.[9] SurfControl provides a 6-page document describing the company's 130-category database.[10] Websense provides an 8-page document describing the company's 80-category database.[11]

Categories are typically safety and liability related, such as "Pornography", "Gambling," and "Hacking;" or productivity and appropriate use related, such as "Sports," "Entertainment," and "Shopping."

Most filtering software databases are delivered by software that offers a high degree of flexibility, allowing organizations to select one or more of dozens of categories for blocking, monitoring, or warning. An example is the SmartFilter program, which offers "30 individual categories of Web sites" with the ability to "Deny, allow, coach (warn, but allow), delay, or report only."[12] A screen shot of the administrative interface that allows this functionality is shown below:



ns-Usenet News
nd-Nudity
nw-Gen. News
oc-Cults/Occult
os-Online Sales
po-Politics/Religion
pp-Personal
ps-Portal Sites
sh-Self Help/Health
sp-Sports
sx-Sex
tr-Travel
u0-User defined category 0
u1-User defined category 1
u2-User defined category 2
u3-User defined category 3
u4-User defined category 4
u5-User defined category 5
u6-User defined category 6
u7-User defined category 7
u8-User defined category 8
u9-User defined category 9
wm-Webmail

| | Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|---|---|---|---|---|---|---|---|
| 0:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 1:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 2:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 3:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 4:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 5:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 6:00 | ALLOW | DELAY | DELAY | DELAY | DELAY | DELAY | ALLOW |
| 7:00 | ALLOW | DELAY | DELAY | DELAY | DELAY | DELAY | ALLOW |
| 8:00 | ALLOW | DENY | DENY | DENY | DENY | DENY | ALLOW |
| 9:00 | ALLOW | DENY | DENY | DENY | DENY | DENY | ALLOW |
| 10:00 | ALLOW | DENY | DENY | DENY | DENY | DENY | ALLOW |
| 11:00 | ALLOW | DENY | DENY | DENY | DENY | DENY | ALLOW |
| 12:00 | ALLOW | COACH | COACH | COACH | COACH | COACH | ALLOW |
| 13:00 | ALLOW | DENY | DENY | DENY | DENY | DENY | ALLOW |
| 14:00 | ALLOW | DENY | DENY | DENY | DENY | DENY | ALLOW |
| 15:00 | ALLOW | DENY | DENY | DENY | DENY | DENY | ALLOW |
| 16:00 | ALLOW | DENY | DENY | DENY | DENY | DENY | ALLOW |
| 17:00 | ALLOW | DELAY | DELAY | DELAY | DELAY | DELAY | ALLOW |
| 18:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 19:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 20:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 21:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 22:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |
| 23:00 | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW | ALLOW |

## The Social Benefits of Filtering Software

Driving the rapid growth of the filtering industry are the social benefits that result from the use of filtering software in homes, schools, and organizations. Congress recognized the benefits of promoting a vigorous filtering industry in 1996 when it enacted "Good Samaritan" immunity from "private blocking and screening of offensive material" in the Telecommunications Act of 1996. The text of act states:

> *`(b) POLICY- It is the policy of the United States--*
>
> *`(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;*
>
> *`(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;*
>
> *`(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;*
>
> *`(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material*[13]

The industry analyst Frost & Sullivan in 2001 identified six market drivers of the filtering industry. It is not coincidental that these market drivers are heavily related to social benefits:[14]

*Key drivers for the U.S. content filtering market are:*

- *Lack of Internet Regulation*
- *Limit Legal Liability*
- *Prevention of Exposure of Adult Material to Children*
- *Legislative Action*
- *Preservation of Corporate Bandwidth*
- *Increase Employee Productivity*

As the Frost & Sullivan report points out, "lack of Internet regulation" and the desire for the "prevention of exposure of adult material to children" are the most obvious social benefits of filtering software. The threat posed to children by Internet pornography and other Internet dangers is not imaginary. According to the Kaiser Family Foundation, 70% of teens have accidentally stumbled across pornography online.[15]

These accidental exposures occur because, among other reasons, the Internet if full of misleading pornography websites that lure children. The research firm Cyveillance documented over 19,000 examples of pornographers disguising their sites with common brand names, including Disney, Barbie, ESPN, etc., which can entrap children.[16] The harm done to children by these exposures was documented in a report by the National Center for Missing and Exploited Children, which found that of children accidentally exposed to online pornography, "23% were very or extremely upset by the exposure."[17]

These disturbing statistics have led to the widespread adoption of filters in homes and schools, and surveys show that educators, parents, and the teenagers themselves all strongly support the use of filters. According to the Digital Media Forum, "92% of all Americans said pornography should be blocked on school computers."[18] A survey by the Association for Supervision and Curriculum Development found that "90% of educators surveyed favored the installation of blocking software on school computers to prevent student access to potentially inappropriate or offensive Web sites."[19] Finally, the Kaiser Family Foundation found that "63% of 15-to 17- year olds say they favor the use of filters in their schools." [20]

Beyond protecting children, the social benefits of filtering software extend to the workplace as well. As the Frost & Sullivan report shows, the desire for organizations to "limit legal liability," "increase employee productivity," and the "preservation of corporate bandwidth" are all desired social benefits that drive the adoption of filtering software.[21]

Again, research documents the problem. According to the Center for Internet Studies, more than 60% of companies have disciplined – and more than 30% have terminated – employees for inappropriate use of the Internet. [22] According to the American Management Association, 27% of Fortune 500 companies have battled sexual harassment claims stemming from employee misuse and abuse of corporate e-mail and Internet systems. [23]

## The Evolution of Filtering Industry Markets

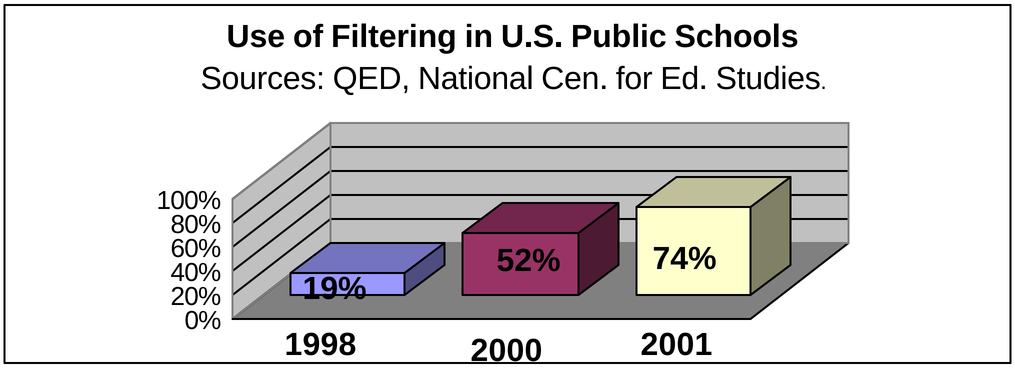
Internet filtering software appeared in 1995 after a series of articles, including a cover story in Time Magazine[24] documented the widespread availability of Internet pornography, and in particular the danger posed to children with Internet access. During the summer of 1995, a filtering software industry appeared with the release of products designed for parents such as CyberSitter[25], Cyber Patrol[26], and SurfWatch[27].

The new filtering industry received a significant boost in 1997, when the United States Supreme Court struck down the Communications Decency Act (CDA) as unconstitutional. The CDA required Internet sites to block "indecent" material, and the Court pointed to filtering software as a less restrictive means for controlling access to pornography on the Internet.[28] The years since that 1997 decision have led to steady growth in the use of software filters. According to the latest research, in the year 2001, 74% of public schools[29], 43% of public libraries[30], 40% of major U.S. corporations[31], and 41% of Internet-enabled homes with children[32] have adopted filtering software.

The adoption of filtering software in the U.S. has followed a similar pattern in businesses, schools, homes, and libraries. Industry analysts predict that the global filtering market, valued at $270 million in 2002, will grow to $729 million by 2006[33]

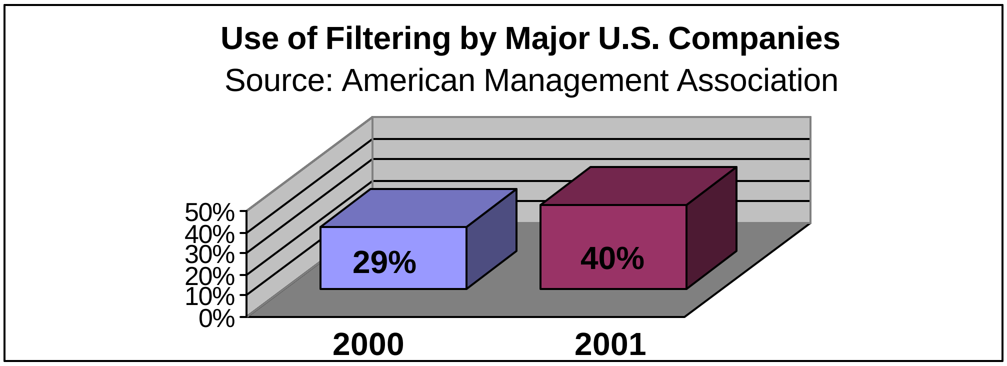
### Schools

The most dramatic growth has occurred in public schools. In May 1998, Quality Education Data surveyed school districts with Internet access and found that for the 1998 school year, 19% of schools were using filters.[34] Just one year later, QED found that the use of filters had increased to 52.5%.[35] The most recent data on school filter use comes from a May 2001 study by the National Center for Education Studies, which found 74% of public schools are now using filtering software.[36]



### Major Corporations

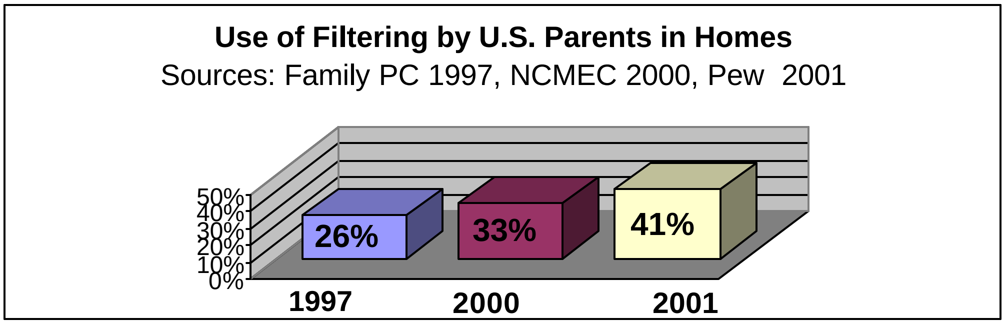
In 2000, the American Management Association surveyed major U.S. companies and found that "29 percent block Internet connections to unauthorized or inappropriate Web sites." [37] In a similar survey one year later, the AMA found that number had grown to 40%.[38]


Use of Filtering by Major U.S. Companies

Source: American Management Association

**Homes with Children and Internet Access**

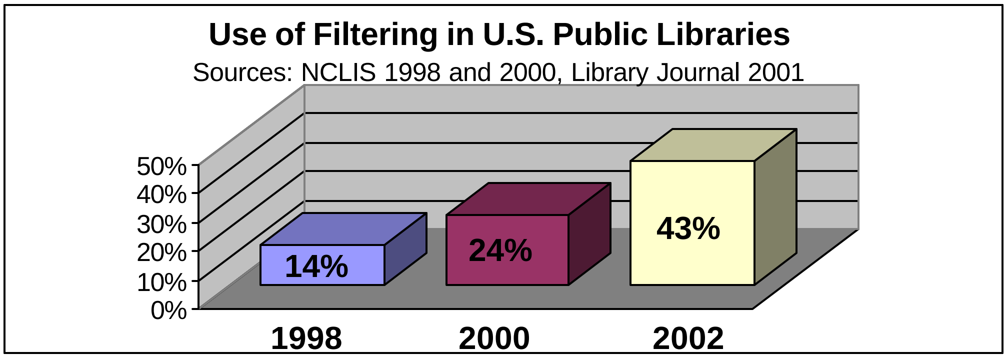
A 1997 survey of parents on the Internet, by Family PC found that "26 percent used some form of parental-control software."[39] A 2000 study by the National Center for Missing and Exploited Children found the number had increased to 33 percent.[40] The Pew Internet and American Life Project reported in June of 2001 that filtering by parents had increased to 41 percent. [41]


Use of Filtering by U.S. Parents in Homes

Sources: Family PC 1997, NCMEC 2000, Pew  2001

**Public Libraries**

The National Commission on Library and Information Science surveyed public libraries in 1998, and found that 14 percent were using filters[42]. By 2000, NCLIS conducted a second survey that found the number had risen to 24 percent. [43] Near the end of 2001, Library Journal conducted a survey that found the number had increased to 43 percent. [44]


Use of Filtering in U.S. Public Libraries

Sources: NCLIS 1998 and 2000, Library Journal 2001

## For Economic and Social Reasons, Filtering Companies Do Not Publish Their Databases in the Entirety

Filtering companies do not publish their entire databases, all at once, in a single publicly available form. There are three reasons for this; filtering databases are considered proprietary, filtering companies want to protect their investment, and filtering companies want to protect children.

### Filtering databases are considered proprietary.

Filtering databases are, like many other databases, considered proprietary because of the original content and arrangement created for the databases. The Copyright Office acknowledged that databases are entitled to copyright protection under the DMCA in the 2000 *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, when the Copyright Office rejected arguments to grant an exemption to circumvent the copyright protection measures for "thin copyright" databases*:*

> *Most often this argument is made in the context of databases that contain a significant amount of uncopyrightable material. These databases may nonetheless be covered by copyright protection by virtue of the selection, coordination and arrangement of the materials. They may also incorporate copyrightable works or elements, such as a search engine, headnotes, explanatory texts or other contributions that represent original, creative authorship.*[45]

Filtering databases, consisting of uncopyrightable material (publicly available URLs), selected and arranged with copyrightable material (subject classification schemes), fit neatly into the "thin copyright" category.

The practice of not allowing full access to the entire database has long been standard among many database providers. Like filtering database companies, other large vendors of databases and search engines also recognize the economic necessity of copyright controls, and forbid access except through query interfaces.

The "General Terms and Conditions for use of the LexisNexis Services" forbids use of the database other than through the querying interface:

> *… you are prohibited from downloading, storing, reproducing, transmitting, displaying, copying, distributing, or using Materials retrieved from the Online Services. You may not print or download Materials without using the printing or downloading commands of the Online Services.*[46]

The license agreement for large database vendor Dialog is even more explicit in forbidding circumventions:

> *Subscriber will not modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Profound Software used to access the Profound Service via the internet.*[47]

### Filtering companies want to protect their investments

As is clear from the labor-intensive process described by Mr. Ophus in the section on page 7, "About Filtering Databases", the compilation of filter databases is extraordinarily expensive and labor intensive. The databases of the larger filtering companies contain millions of entries. N2H2's database contains four million entries[48], SurfControl's database contains 5 million entries[49], and 8e6's database contains 2.8 million entries.[50] Websense estimates they have invested "40 man-years of classification"[51] to build a database of 4 million entries.[52]

In addition to the enormous labor costs, there are considerable requirements to create the technology infrastructure required to create and maintain such databases. The total "ramp up" cost of creating a top-quality filtering database of millions of entries is in the tens of millions of dollars. If such databases were published, the loss would be enormous. A start-up "parasite company" could steal this valuable data, and immediately launch its own filtering product without having to spend these "ramp up" costs. These "parasite companies" would be at a huge economic advantage, as they would not incur the staggering costs of database creation.

One measure of the value filtering companies place on their databases is the direct correlation between filtering database size and the use of copyright protection measures. All of the filtering companies that use URL databases employ copyright protection to protect their databases from economic parasitism, with the exception of Net Nanny, which publishes its database[53]. All of these same filtering companies have databases with hundreds of thousands or millions of entries, with the exception of Net Nanny, which has a database of just 2,000 websites.[54] With a database so small -- less than 1% of the size of the databases used by Websense, Surfcontrol, N2H2, and 8e6 Technologies, it is clear that Net Nanny has little intellectual property to protect. It is not surprising that Net Nanny recently declared bankruptcy.[55]

Another indication of how valued filtering databases are is the fact that many of the filtering companies build marketing campaigns around the quality of their databases, and the studies which show a filtering company's database to be superior to others are highly prized as marketing tools. In 2002, Websense launched a "Why Quality Matters" marketing campaign based on a study by eTesting Labs that found the Websense database superior to several competitors.[56] N2H2 has issued two press releases based on favorable study results, including a test by eTesting Labs[57] and another test by the Kaiser Family Foundation.[58]

At this writing, the nation's two largest Internet service providers, American Online (AOL) and the Microsoft Network (MSN), are engaged in a fierce competition for home Internet subscribers. Each is spending millions of dollars on television ad campaigns that focus on the filtering databases used in the companies' parental controls. From a November 12, 2002 story in The Washington Post:

> *America Online and Microsoft understand, too, which is why the giant Internet service providers are locked in a battle to attract parents concerned about online security. In recent weeks, each has started hawking new sets of parental controls -- AOL 8 and MSN 8, respectively -- to ease the minds of parents who want their children to have access to the infinite world of the Internet but not its infinite dangers. Of course, each company is hoping to win subscribers in the process.*[59]

Again, in the 2000 *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies,* the Copyright Office recognized this basic economic fact, and acknowledged the potential devastation to database publishers, when the Copyright Office refused to grant an exemption for "thin copyright" databases:

> *Access controls provide an increased incentive for database producers to create and maintain databases. Often, the most valuable commodity of a database producer is access to the database itself. If a database producer could not control access, it would be difficult to profit from exploitation of the database. Fewer databases would be created, resulting in diminished availability for use.*[60]

**Filtering companies want to protect children**

Lastly, there is a huge potential for damage to children by the publication of filtering databases. A child with access to a filtering database would have ready access to a huge list of pornographic and other harmful websites. This situation is not hypothetical. Net Nanny, the lone filtering company that publishes its database, suffered a disastrous marketing experience that needlessly exposed countless children to pornography as a result of publishing its database. From a June 22, 2000 news story published in *The London Telegraph:*

> *BURGER KING has been forced to withdraw a CD-Rom given away with children's meals this week after complaints that the disc contained internet addresses for more than 2,000 pornographic websites.*
>
> *The restaurant chain, which has 630 stores in the UK, acted after customers complained that their children could have easily accessed the addresses, which include sex-related internet discussion groups and hardcore pornographic websites. More than one million CDs had been given away before the promotion was pulled on Monday, according to Burger King.*
>
> *Anyone purchasing a children's meal since the offer began more than two weeks ago would have received a CD supplied to Burger King by the internet service provider <KZuk.net>, which offers secure internet usage for children.*
>
> *The CD includes software called Net Nanny, designed to provide parents with a filtering mechanism to block certain websites. Unfortunately, once installed from the CD, it only takes a couple of mouse clicks to view the global list of pornographic web addresses.*[61]

The filtering companies that employ copyright protection for their databases have much larger lists of pornographic websites. Surfcontrol's database has "more than 600,000 containing sexually explicit content."[62] Were such a list to be made readily available to children, the damage to children could be significant.

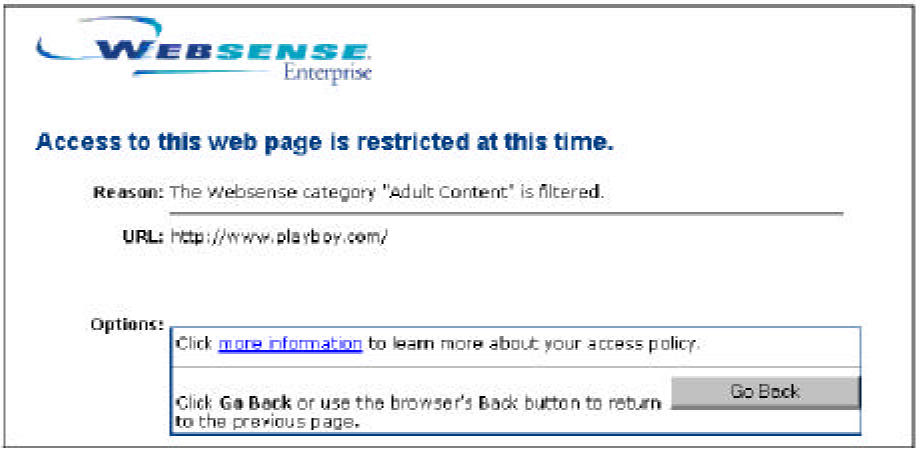
The violation of copyright protection for filtering databases involves not simply the loss of intellectual property and the diminished availability of a valuable resource, but the safety of children around the world. Therefore, the reasons for refusing an exemption to filtering databases are even more compelling than they are for databases such as LexisNexis and Silver Platter, which the Copyright Office has denied requests for exemption to allow the circumvention of copyright protection measures.

### Filtering Companies Provide Free Access to their Databases Through Querying Interfaces and Trial Copies

Because of the compelling social and economic reasons described above, filtering companies do not provide unlimited public access to their databases. However, this has not prevented researchers from evaluating and criticizing filtering databases. Nearly all filtering companies allow anyone to download a trial copy of the filtering software and accompanying database for a 30-day evaluation. [63]

In most cases, a trial version of a filtering product allows full access to the software's functionality, and allows the user to test if specific websites or groups of websites are categorized by the filtering database.

In most filtering software programs, a user attempts to access a website. If the website is blocked, the software returns a message stating the URL of the blocked website, and the category that caused the website to be blocked. The example below is from the Websense program:



Access to this web page is restricted at this time.

Reason: The Websense category "Adult Content" is filtered.

URL: http://www.playboy.com/

Options:

Click more information to learn more about your access policy.

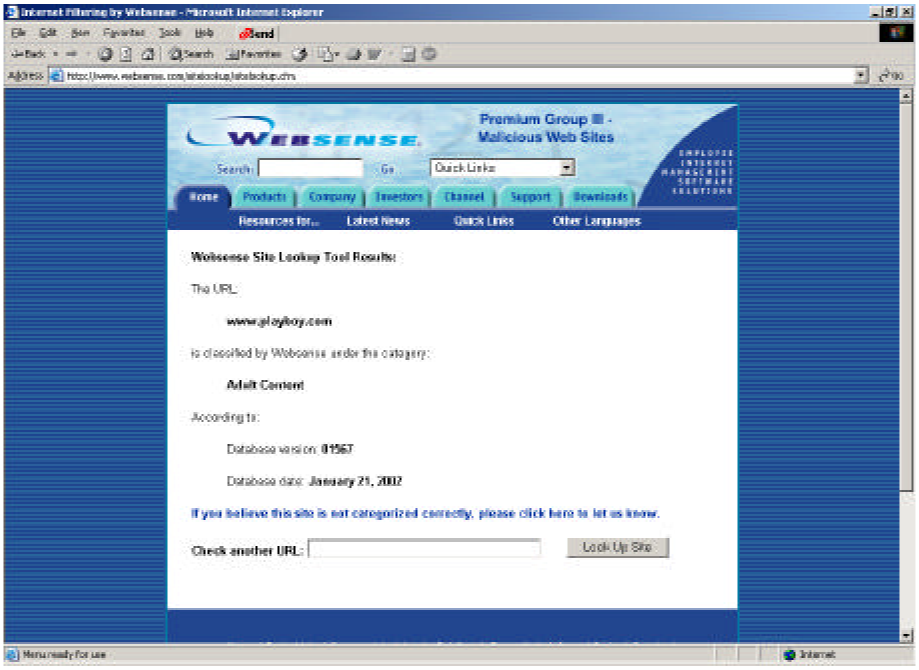
Click Go Back or use the browser's Back button to return to the previous page.

Using this method, a user can assemble a sample of URLs, test them, and record the results. A researcher with basic knowledge of any one of a number of "scripting languages" can configure the software to test a file of website and automatically record the results, thus making the testing of large numbers of URLs relatively easy.

Research and evaluation methods that rely on trial copies of filtering software do require that researchers have the necessary hardware, software, and computer knowledge to download, install, and configure the software.

Recognizing that these requirements are an inconvenience to those who wish to learn about and evaluate filtering databases, a number of filtering companies have taken the step of providing a free, publicly available query interface to their databases. These websites are offered for free on publicly available websites, and allow anyone, anywhere to look up any site, see how it is categorized, and request a "re-review" if they disagree with the categorization.

The *Websense Site Lookup Tool*, available at
http://www.websense.com/sitelookup/sitelookup.cfm
Users may lookup the categorization of any website, and submit a request for re-review.


Internet Filtering by Websense - Microsoft Internet Explorer
File Edit View Favorites Tools Help Send
Back Search Favorites
Address http://www.websense.com/sitelookup/sitelookup.cfm
WEBSENSE
Premium Group III - Malicious Web Sites
EMPLOYEE INTERNET MANAGEMENT SOFTWARE SOLUTIONS
Search: Go Quick Links
Home Products Company Investors Channel Support Downloads
Resources for... Latest News Quick Links Other Languages
Menu ready for use
Internet

Websense Site Lookup Tool Results:

The URL:

www.playboy.com

is classified by Websense under the category:

Adult Content

According to:

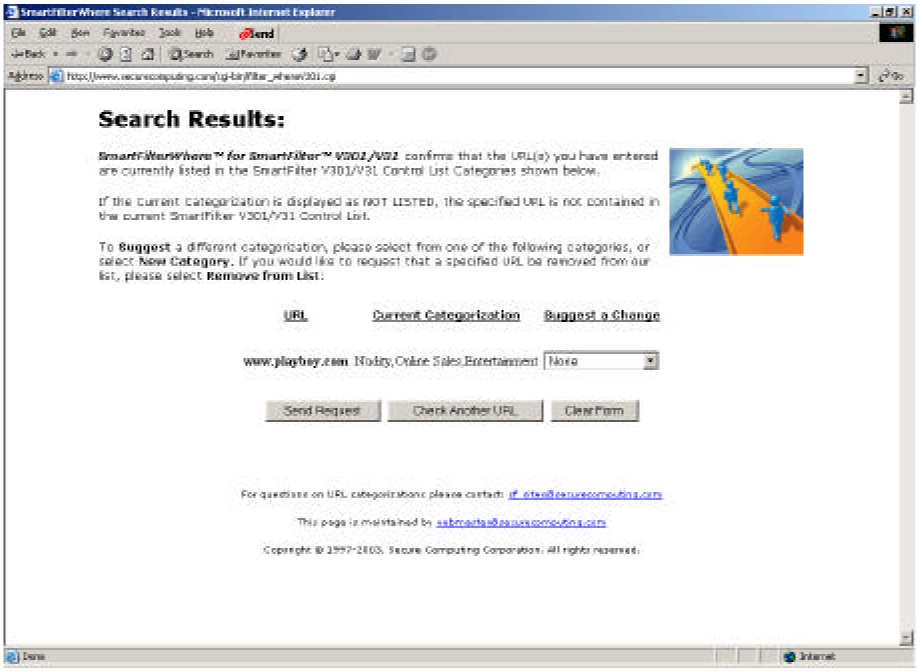
Database version: 01567

Database date: January 21, 2002

If you believe this site is not categorized correctly, please click here to let us know.

Check another URL: Look Up Site

*SmartFilterWhere*, available at www.smartfilterwhere.com
Users may lookup the categorization of any website, and submit a request for re-review.


SmartFilterWhere Search Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help Send
Back Search Favorites
Address http://www.securecomputing.com/cgi-bin/filter_where/301.cgi
Done
Internet

Search Results:

**SmartFilterWhere™ for SmartFilter™ V301/V31** confirms that the URL(s) you have entered are currently listed in the SmartFilter V301/V31 Control List Categories shown below.

If the current categorization is displayed as NOT LISTED, the specified URL is not contained in the current SmartFilter V301/V31 Control List.

To **Suggest** a different categorization, please select from one of the following categories, or select **New Category**. If you would like to request that a specified URL be removed from our list, please select **Remove from List**:

| URL | Current Categorization | Suggest a Change |
|---|---|---|
| www.playboy.com | Nudity,Online Sales,Entertainment | None |

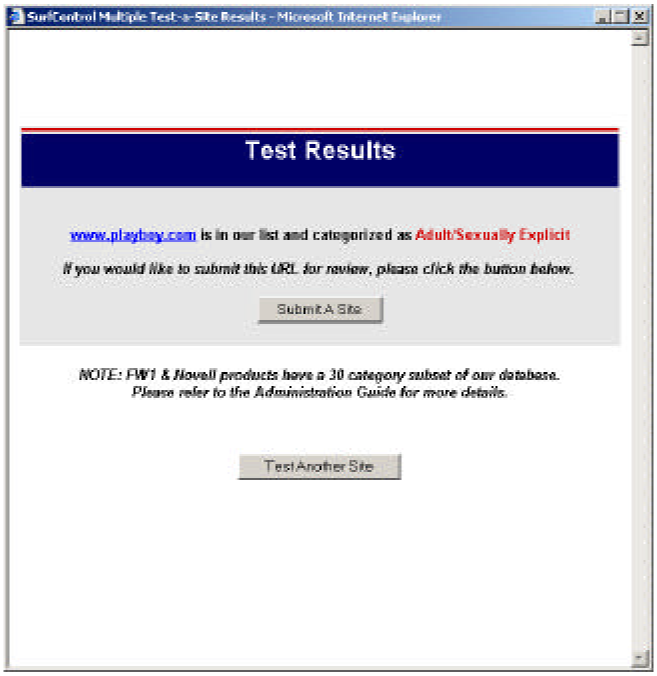
Send Request Check Another URL Clear Form

For questions on URL categorizations please contact: sf_sites@securecomputing.com

This page is maintained by webmaster@securecomputing.com

Copyright © 1997-2003. Secure Computing Corporation. All rights reserved.

*Surfcontrol Test-a-Site*, available at http://mtas.surfcontrol.com/mtas/MTAS.asp
Users may lookup the categorization of any website, and submit a request for re-review.


SurfControl Multiple Test-a-Site Results - Microsoft Internet Explorer
Submit A Site
Test Another Site

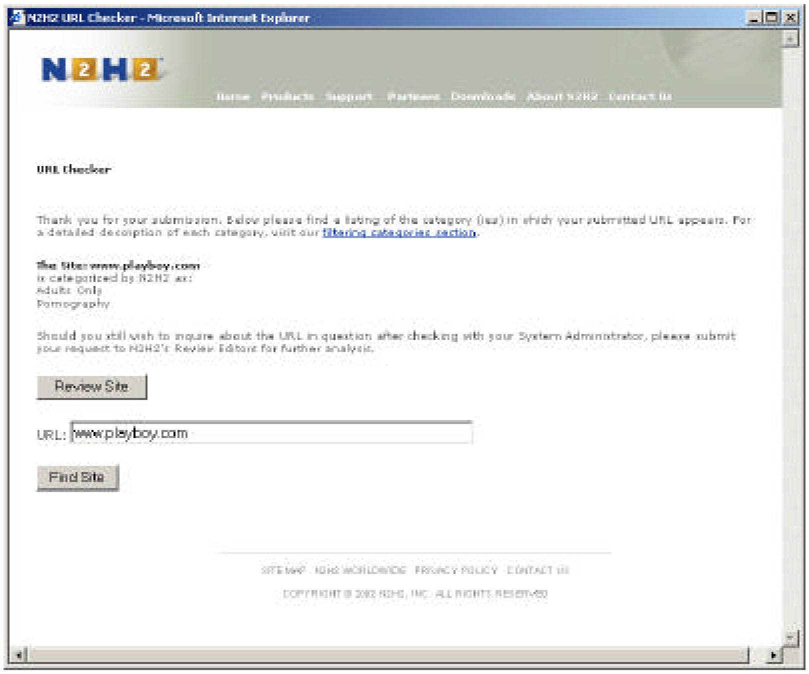
Test Results

www.playboy.com is in our list and categorized as Adult/Sexually Explicit

*If you would like to submit this URL for review, please click the button below.*

*NOTE: FW1 & Novell products have a 30 category subset of our database.*
*Please refer to the Administration Guide for more details.*

*N2H2 URLChecker*, available at http://database.n2h2.com
Users may lookup the categorization of any website, and submit a request for re-review.



URL Checker

Thank you for your submission. Below please find a listing of the category (ies) in which your submitted URL appears. For a detailed description of each category, visit our filtering categories section.

The Site: www.playboy.com
is categorized by N2H2 as:
Adults Only
Pornography

Should you still wish to inquire about the URL in question after checking with your System Administrator, please submit your request to N2H2's Review Editors for further analysis.

URL: www.playboy.com

COPYRIGHT © 2002 N2H2, INC. ALL RIGHTS RESERVED

**Querying is a Well-Established Scientific Method for Evaluating Databases**

Information science establishes a number of measures for evaluating databases. Bert R. Boyce's standard 1994 information science textbook, *Measurement in Information Science* lists a number of database measures, such as scope, attributes, selection of entities, magnitude, timeliness, selectivity, reliability, etc.[64]

Of concern here is the measurement of database retrieval outcomes. Boyce defines a number of formal measures for retrieval outcome, including *relevance, precision,* and *recall.* [65]Boyce then states that "Measures of outcome have traditionally been measures of the relationship between queries or information need statements and retrieved records."[66]

These methods and measures can and have been applied to databases that are not published in their entirety and are only accessible through a query interface. The professional literature of the information science field has a long, rich history of the publication of peer-reviewed research that involves the querying of copyright-protected databases, such as Lexis/Nexis and Dialog.

The examples of such published research are far too many to list for this submission, so only a sampling of such research is provided here. The fact that the databases being evaluated in these studies are, like filtering databases, not accessible in their entirety and are only available through query interfaces does not prevent researchers from using queries to measure their accuracy, including formal information science measures such as *relevance, precision,* and *recall*.

A 1998 publication in the journal *Information Processing & Management* employed querying of the copyright-protected database Lexis/Nexis, and:

> *Compares results of traditional Boolean searching with those of Freestyle, LEXIS/NEXIS's natural language application. Study found that though the Boolean searches had better results more often, neither method demonstrated superior performance for every query, suggesting that different queries demand different techniques.*[67]

1991 master's research published at Kent State University employed querying to evaluate the copyright-protected databases Lexis/Nexis and Westlaw:

> *This paper compares strengths and weaknesses of the Lexis and Westlaw computer assisted legal research systems. Their powerful full text document delivery capabilities are contrasted with their inherent limitations as information retrieval systems. The objective here is to alert users to the complexities of online legal searching and the necessity for evaluating these systems critically. Sample searches highlight the major differences between Westlaw's and Lexis's searching protocols.*[68]

A 2001 article in the *Journal of the American Society for Information Science and Technology* employed querying of the copyright-protected database Dialog, and:

> *Examines the distribution of bibliographic records in online bibliographic databases using 14 different search topics on DIALOG. Discusses the presence of duplicate records and problems with lexical ambiguity, and concludes that the number of databases needed for searches with varying complexities of search strategies is much more topic dependent than previous studies indicated.*[69]

A 1995 article in the journal *Online* employed querying to evaluate the copyright-protected databases Lexis/Nexis and Westlaw:

> *Compares two natural language processing search engines, WIN (WESTLAW Is Natural) and FREESTYLE, developed by LEXIS. Legal issues in natural language queries were presented to identical libraries in both systems. Results showed that the editorials enhanced relevance; a search would be more thorough using both databases; and if only one system were to be used, WESTLAW provides more relative documents.*[70]

A 1992 paper submitted at the *Proceedings of the ASIS Annual Meeting* employed querying to evaluate the copyright-protected databases Lexis/Nexis and Westlaw:

> *Discusses a study in progress that is analyzing retrieval failures in two full-text computer-assisted legal research (CALR) systems, LEXIS and WESTLAW. Computer searching by experts is compared with manual searching by experts, examples are given, and a taxonomy of causes of retrieval failure is discussed.*[71]

Querying methodology has also been extended to newer databases, such as search engines. In this 2002 publication in the *Journal of the American Society for Information Science and Technology*, querying is used to evaluate Google:

> *Compares search effectiveness when using query-based Internet search via the Google search engine, directory-based search via Yahoo, and phrase-based query reformulation-assisted search via the Hyperindex browser by means of a controlled, user-based experimental study of undergraduates at the University of Queensland. Discusses cognitive load, relevance, and search time.*[72]

Filtering databases, being available for searching through query interfaces, fit neatly into a category of databases that can be evaluated using querying methodologies.

## Numerous Laboratory Studies of Filter Databases have Used Querying

There is rich literature dating back to 1995 of laboratory tests of filters using querying methodologies. Among the publications conducting query-based tests have been *Consumer Reports* and *JAMA*. Many of the tests conclude that filters are effective, but others are critical. What the aggregate of these tests show is that filtering databases can be successfully evaluated using querying.

## Journal of the American Medical Association (JAMA) Test

Most recently, the Kaiser Family Foundation conducted a sophisticated test using a querying methodology that was published in the *Journal of the American Medical Association*. One member of the research team that designed the study was a professor at the information school of the University of Michigan, Dr. Paul J. Resnick. The abstract of the study is worth reviewing:

> ***Context*** *The Internet has become an important tool for finding health information, especially among adolescents. Many computers have software designed to block access to Internet pornography. Because pornography-blocking software cannot perfectly discriminate between pornographic and nonpornographic Web sites, such products may block access to health information sites, particularly those related to sexuality.*
>
> ***Objective*** *To quantify the extent to which pornography-blocking software used in schools and libraries limits access to health information Web sites.*
>
> ***Design and Setting*** *In a simulation of adolescent Internet searching, we compiled search results from 24 health information searches (n = 3206) and 6 pornography searches (n = 781). We then classified the content of each site as either health information (n = 2467), pornography (n = 516), or other (n = 1004). We also compiled a list of top teen health information sites (n = 586). We then tested 6 blocking products commonly used in schools and libraries and 1 blocking product used on home computers, each at 2 or 3 levels of blocking restrictiveness.*
>
> ***Main Outcome Measure*** *Rates of health information and pornography blocking.*
>
> ***Results*** *At the least restrictive blocking setting, configured to block only pornography, the products blocked a mean of only 1.4% of health information sites. The differences between blocking products was small (range, 0.6%-2.3%). However, about 10% of health sites found using some search terms related to sexuality (eg, safe sex, condoms) and homosexuality (eg, gay) were blocked. The mean pornography blocking rate was 87% (range, 84%-90%). At moderate settings, the mean blocking rate was 5% for health information and 90% for pornography. At the most restrictive settings, health information blocking increased substantially (24%), but pornography blocking was only slightly higher (91%).*
>
> ***Conclusions*** *Blocking settings have a greater impact than choice of blocking product on frequency of health information blocking. At their least restrictive settings, overblocking of general health information poses a relatively minor impediment. However, searches on some terms related to sexuality led to substantially more health information blocking. More restrictive blocking configurations blocked pornography only slightly more, but substantially increased blocking of health information sites.*[73]

### Consumer Reports Tests

In May 1997, Consumer Reports, using querying methods, tested four home filters, CyberSitter, Net Nanny, SurfWatch, and Cyber Patrol. Consumer Reports recommended none of the filters, and concluded:

> *We set each to maximum protection, then noted its ease of use and effectiveness in keeping us from viewing 22 easy-to-find web sites we had judged inappropriate for children…None is totally effective.*[74]

In March 2001, Consumer Reports, again using querying methods, issued a second evaluation of filtering software. Consumer Reports evaluated AOL Parental Controls, Cyber Patrol, Cyber Sitter, Cyber Snoop, Internet Guard Dog, Net Nanny, and Norton Internet Security 2001. Consumer Reports concluded:

> *Filtering software is not a substitute for parental supervision. Most of the products we tested failed to block one objectionable site in five.* [75]

### ZDNet Lab Tests for PC Magazine

PC magazine is probably the best known, and among the most highly regarded sources of software testing. Since 1982, PC Magazine has published thousands of software tests. PC Magazine's test laboratory, ZDNet Labs, is described as performing "Comprehensive performance and functionality testing. Our objective, precise, and repeatable testing methods--utilizing benchmarks accepted by the industry."[76]

PC Magazine has conducted more formal testing of filters than any other publication. The testing laboratories employed by PC Magazine conducted eight rounds of testing multiple filters from 1995 to 2001. Several of these tests clearly describe the use of querying methods.

In March of 1998, PC Magazine had ZDNet Labs test filtering software blocking effectiveness. Ten products were tested: Cyber Patrol, Cyber Sentinel, Cyber Snoop, Cyber Sitter 97, Net Nanny, SurfWatch,Time's Up!, WatchDog, WebChaperone, and X-Stop. PC Magazine provided a summary:

> *Our tests involved trying to access extensive lists of URLs, words, and phrases while using each of the products. We tried to access well-known pornography sites as well as less obviously objectionable sites, some of which made no reference to sex…Our testing confirms that these packages principally block sites with pornography, obscenity, and sexually explicit content--and they do a pretty good job.*[77]

In May 1999, PC Magazine tested filters, this time with an emphasis on business products, testing Cyber Patrol, Little Brother Pro, SmartFilter, and Websense. In this test, ZDNet Labs used a querying method and "created a list of 100 URLs in nine categories and then tried to browse them through these products," and concluded:

> *The software packages in this roundup have matured as the demand for them has increased--and in more ways than the addition of productivity categories… All in all, these products delivered as advertised, though some do so with more panache than others.*[78]

Another PC Magazine test occurred in the September 2001 issue. This was the most extensive test to date, involving twelve filters: AOL Parental Control, CyberSitter, CyberSnoop, Internet Guard Dog, Net Nanny, Norton Internet Security, IM Web

Inspector, Super Scout, Surfin Gate, 8e6, Iprism, and NetSpective. PC Magazine used a querying methodology and concluded:

> *In testing, most products blocked more than 85 percent of objectionable content—good enough to make a serious dent in inappropriate Internet usage.*[79]

### Info World Test Center Tests for Info World Magazine

Info World is one of the leading technology publications, and provides "in-depth technical analysis on key products, solutions, and technologies for sound buying decisions and business gain."[80] Like PC Magazine, Info World conducts regular software testing through a professional testing laboratory, the InfoWorld Test Center:

> *The InfoWorld Test Center differentiates itself by providing the most real-world approach to testing. Our tests, which are conducted by the most knowledgeable analysts in the industry, focus on products and solutions as they are used and exist in IT environments.*[81]

From 1997 to 2000 the InfoWorld Test Center conducted four tests of filtering software blocking effectiveness. Two tests clearly describe the use of querying methods. In the August 1997 issue, InfoWorld tested WebSense, and found that, "Every time I tried to access a blocked site, I was presented with my customized "access denied" message."[82] In February 1998, InfoWorld tested Cyber Sentinel, and concluded, "Cyber Sentinel proved quite adept at flagging all of my attempts at accessing offensive material."[83]

### PC World Test Center Tests for PC World

PC World is the world's largest computer magazine, with a readership of nearly 6.9 million. Like PC Magazine, PC World has conducted thousands of software tests through its testing laboratory, the PC World Test Center. PC World conducted two tests of filtering effectiveness in 1997 and in 2001. One test clearly describes the use of querying methods.

In October 1997, PC World tested five home filters --SurfWatch, Cyber Patrol, CyberSitter, Net Nanny and Net Shepherd:

> *Internet-blocking software is neither as easy to use nor as foolproof as parents and developers would like…Among the five programs we tested, two (Cybersitter and SurfWatch 1.6) effectively filtered out all 10 of our bellwether adult-oriented pages."*[84]

### ZDNet Lab Test for Internet Magazine

In December 1997, ZD Internet Magazine used the ZD Net testing labs to measure the effectiveness of eight filters: Bess, Cyber Patrol, CyberSitter,SafeSurf, SurfWatch, WebSense, X-Stop and Cyber Snoop. ZD Net Labs used a querying methodology and found the majority of them effective. Internet Magazine reported that SafeServer and CyberSnoop were less effective, but did find the majority of the products effective:

> *During our tests, Bess performed well, blocking all the pornographic and objectionable sites on our test list.*
>
> *In our testing, Cyber Patrol performed fairly well, blocking access to most of the sites on our list. All the pornographic sites were blocked effectively.*
>
> *During our testing, CYBERsitter 97 blocked access to most of the pornographic sites on our testing list.*

> *SurfWatch was the best performer on our site-blocking test, blocking access to all the pornographic sites we tested, as well as adequately blocking attempts to search for obscene words with Yahoo! and other search engines.*
>
> *In our tests, WebSENSE performed exceptionally well.*
>
> *In our site blocking tests, X-Shadow performed quite well, preventing access to almost all the pornographic sites, as well as preventing searches on obscene words.*[85]

**Network World Test Alliance Tests for Network World**

Another well-known technology publication, Network World, conducted a round of filter tests through its Network World Test Alliance network of testing labs. Network World frequently tests software, and is described as "the premier source of objective, authoritative reviews in the network market."[86] Network World used a querying methodology and tested seven filters: LittleBrother Pro, WebSense, WizGuard, SOS, and NNPro. Network World found that "All the products with predefined databases allow you to customize their lists, but we found that locating inappropriate sites the vendors didn't include was a challenge." [87]

**Real-World Labs Test for Network Computing**

Network Computing is another leading technology publication that regularly tests software. As described on the company website, "Network Computing performs hands-on product reviews in our Real-World Labs co-located on the sites of two large universities, a Fortune 100 corporation, as well as bench-test facilities."

Real-World Labs, using a querying methodology, tested SurfControl Super Scout, Elron Internet Manager, Little Brother, SmartFilter, Iprism, WebSense, and N2H2:

> *We installed and configured each product to monitor and block Web traffic on our production network. We then configured each product to block traffic to unproductive or "improper" sites while letting productive uses of Web, e-mail and FTP traffic go past…We visited a broad range of improper Web sites to evaluate each product's content policies and, if applicable, dynamic policy rules.*
>
> *Our test results showed that network administrators can choose from many effective content-monitoring solutions capable of stifling the most adamant of browsers.*[88]

**eWeek Labs Test for eWeek**

Another popular technology publication is eWeek, which regularly tests software through the eWeek Labs. In the February 2001 issue, eWeek Labs tested the effectiveness of SmartFilter using a querying methodology, and concluded that, "We were impressed with the quick response from SmartFilter when we tried to access Web sites that were in the "Deny" ACL.[89]

**IW Labs for Internet World**

Since 1995, Internet World has been one of the leading Internet technology publications, and regularly tests Internet software in IW Labs. In September 1996, Internet World usad a querying methodology and examined Intergo, Cyber Patrol, Net Nanny, Net Shepherd, Specs for Kids, CyberSitter, and Surfwatch:

> *To evaluate how well the current programs work, IW Labs rounded up every available commercial product and tested them under controlled laboratory conditions…While each of the products is sold for the explicit purpose of blocking objectionable material, only three (Cyber Patrol, InterGo, and Specs for Kids) are able to do that with reasonable certainty.*

| | Inter go | Cyber Patrol | Net Nanny | Net Shep | Specs for Kids | Cyber sitter | Surf watch |
|---|---|---|---|---|---|---|---|
| Drugs | Excellent | Excellent | Poor | Fair | Excellent | Fair | Good |
| Sex | Excellent | Excellent | Fair | Fair | Excellent | Good | Poor |
| Violence | Excellent | Excellent | Poor | Fair | Excellent | Excellent | Poor |

Ratings reflect the success of each product in blocking three main categories of objectionable material based on 100 test sites using the package's most stringent level of controls.[90]

**ETesting Labs**

The U.S. Department of Justice commissioned eTesting Labs to compare the four leading institutional-grade Web content filtering applications for effectiveness at blocking 200 randomly selected URLs containing pornography.[91] The test was submitted at the trial, and published in April 2002. Another eTesting Labs test was conducted for Websense. eTesting Labs tested 6,600 URLs for both over blocking and under blocking. The results were published in March 2002.[92]

**Log File Analysis**

Yet another method of evaluating filters without circumventing copyright protection is log file analysis. Most filtering products generate log files during their use. A log file records all Internet access by users, including URL, time, date, and the IP address of the workstation. When an attempt to access a URL is blocked by the filters, the log file also records this. Analyzing log files offers the advantage that the sample is based on real use.

Only a small number of filter log file studies have been done to date, and this is likely because there are significant technical hurdles to properly analyzing and processing large log files, which can often run to millions of entries. Two such studies were presented in the case ALA v. U.S., by Certus Consulting Group[93] and by Tacoma Public Library Central Library Manager David Biek[94]

## Courts have Evaluated Filter Databases Without Research Derived from Circumventing Copyright Protections

To date, three trial courts have directly evaluated filtering software, and issued findings of fact and of law based on those evaluations. Notably, not one of these courts has used research derived from the circumvention of copyright protection to reach these conclusions. Further, none of these courts has opined that the use of copyright protection measures is in any way an impediment to reaching findings of fact and of law pertaining to the use of filtering software.

### ACLU v. Reno I

The first court to examine the effectiveness of filters was ACLU v. Reno[95] in 1996, which involved the Communications Decency Act (CDA), an act that required Internet sites to filter indecent speech. The Reno court heard testimony from the Ann Duvall, the president of the Surfwatch filtering company[96], examined filters, and drew conclusions about filter effectiveness as part of the court's justification for striking down the CDA:

> *73. Despite its limitations, currently available user-based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available." 12*
>
> *[Footnote 12:] Testimony adduced at the hearing suggests that market forces exist to limit the availability of material on-line that parents consider inappropriate for their children. Although the parties sharply dispute the efficacy of so-called "parental empowerment" software, there is a sufficiently wide zone of agreement on what is available to restrict access to unwanted sites that the parties were able to enter into twenty-one paragraphs of stipulated facts on the subject, which form the basis of paragraphs 49 through 69 of our Findings of fact. Because of the rapidity of developments in this field, some of the technological facts we have found may become partially obsolete by the time of publication of these Findings.*[97]

Nowhere in the Reno I court's decision is there any suggestion that the use of copyright protection circumvention of filtering databases posed any impediment to the court's evaluation of filtering.

### ACLU v. Reno II

The second court to examine the effectiveness of filters was ACLU v. Reno II in 1998.[98] ACLU v. Reno II is a still ongoing challenge to the constitutionality of the Children's Online Protection Act (COPA), a successor to the CDA. Again, the trial court evaluated the effectiveness of filtering software. Again, nowhere in the Reno II court's decision is there any suggestion that the encryption of filtering databases posed any impediment to the court's evaluation of filtering:

> *The plaintiffs suggest that an example of a more efficacious and less restrictive means to shield minors from harmful materials is to rely upon filtering and blocking technology.(6) Evidence was presented that blocking and filtering software is not perfect, in that it is possible that some appropriate sites for minors will be blocked while inappropriate sites may slip through the cracks. However, there was also evidence that such software blocks certain sources of content that COPA does not cover, such as foreign sites and content on other protocols. (Finding of Fact 66). The record before the Court reveals that blocking or filtering technology may be at least as successful as COPA would be in restricting minors' access to harmful material online without imposing the burden on constitutionally protected speech that COPA imposes on adult users or Web site operators. Such a factual conclusion is at least some evidence that COPA does not employ the least restrictive means.*[99]

**American Library Association v. U.S.**
The third court to examine filter databases was ALA v. U.S.,[100] which challenged the constitutionality of the Children's Internet Protection Act (CIPA), a federal law that requires schools and libraries that receive certain types of federal funding to purchase filtering software.

The ALA court heard extensive testimony from a number of experts about the effectiveness of filtering software. Six witnesses conducted and presented research that evaluated filter effectiveness. Four of these witnesses used querying methodologies, and two used log file analysis. Notably, none of the experts used research methods that employed the circumvention of copyright protection to examine filters.

**Plaintiff witness Dr. Geoff Nunberg**
Dr. Nunberg used a querying method when he reviewed 250 to 300 sites to compile a set of 29 "illustrative" examples of wrongly blocked sites, and was able to identify 29 sites, or 10% of his "potentially incorrect" set, that were, in fact, incorrectly blocked. [101]

**Plaintiff witness Benjamin Edelman**
Mr. Edelman used a querying method when he tested approximately 550,000 pages in order to generate a list of 6,000 to 7,000 pages that "may" be overblocked. Four librarians then reviewed samples of this list.[102]

**Plaintiff witness Christopher Hunter**
Mr. Hunter used a querying method when he created a sample of 200 sites which he tested against several filters. [103]

**Defense witness Christopher Lemmons**
Mr. Lemmons of eTesting Labs used a querying method when he compared the four leading institutional-grade Web content filtering applications for effectiveness at blocking 200 randomly selected URLs containing pornography. [104]

**Defense witness Cory Finnell**
Certus Consulting Group collected actual filtered Internet log file data from three public library systems. Certus found filtering error rates of between 6.34% and 8.14%.[105]

**Defense witness David Biek**
Tacoma Public Library Central Library Manager David Biek submitted an analysis of Cyber Patrol log files. Based upon his review of a sample of the January 2000 intercept logs, Mr. Biek concluded that the CyberPatrol filter flagged sites at a rate of approximately 98% conformity with the category definitions used by the filtering software.[106]

### The ALA Court's Decision

In the ALA decision, the court noted that:

> *The only way to discover which URLs are blocked and which are not blocked by any particular filtering company is by testing individual URLs with filtering software, or by entering URLs one by one into the "URL checker" that most filtering software companies provide on their Web sites.*[107]

The court went on to discuss the problems associated with evaluating filters, noting: "The fundamental problem with calculating over- and underblocking rates is selecting a universe of Web sites or Web pages to serve as the set to be tested." The court suggested the preferred method would be "a truly random sample of the indexed Web"[108] The court, fully aware of the encrypted nature of filtering databases, discusses methods for evaluating filters, cites a preferred method, and pointedly does not cite the encryption of filtering databases as a barrier to filter research.

The court concluded its evaluation of filters by noting:

> *Those public libraries that have responded to these problems by using software filters have found such filters to provide a relatively effective means of preventing patrons from accessing sexually explicit material on the Internet. Nonetheless, out of the entire universe of speech on the Internet falling within the filtering products' category definitions, the filters will incorrectly fail to block a substantial amount of speech.* [109]

### Mainstream Loudoun v. Board of Trustees

*Mainstream Loudoun v. Board of Trustees* involved the constitutionality of a public library's filtering policy using the software program X-Stop. However, the Loudoun court did not address the effectiveness of filtering software, noting, "…our finding that the Policy is unconstitutional on its face makes any consideration of the operation of X-Stop moot."[110]

## Government Commissions have Evaluated Filter Databases Without Research Derived from Circumventing Copyright Protections

Two important government commissions have examined the effectiveness of filtering software. In both cases, the commissions received testimony from filtering companies, as well as testimony from interest groups promoting filters and interest groups opposed to filters. Both commissions came to conclusions about the effectiveness of filters. Notably, both commissions failed to conclude that copyright protection mechanisms represent a significant barrier to the evaluation of filter databases.

### National Research Council

In November 1998, the U.S. Congress mandated a study by the National Research Council (NRC) to address the availability of pornography on the Internet. In response to this mandate, the National Academies formed a committee with expertise diverse enough to address this topic. After a hearing from a diverse body of commenters on the subject of filtering effectiveness, and conducting site visits to schools and libraries where filters were in use, the committee issued a lengthy report in May 2002 entitled *Youth, Pornography, and the Internet*. The report issued a number of findings, including findings regarding the effectiveness of filtering software:

> *Filters--systems or services that limit in some way the content to which users may be exposed--are the most-used technology-based tool. [Section 12.1] All filters suffer from both false positives (overblocking) and false negatives (underblocking). However, filters can be highly effective in reducing the exposure of minors to inappropriate content if the inability to access large amounts of appropriate material is acceptable.*[111]

The NRC report contains an extensive discussion of methods for evaluating filters. Notably, the report does not state that copyright protection measures are a barrier to research, and echoes the sentiments of the ALA v. U.S. court as to the choice of methods for evaluating filter databases:

> *A controversy over methodology was the subject of testimony to the committee. One approach is that the number of appropriate pages should be estimated on the basis of a random sampling of Web pages. A second approach is that the number should be estimated on the basis of actual usage, which weights certain popular Web pages more heavily than those not accessed as frequently.*[112]

### The COPA Commission

In October 1998 Congress enacted the Child Online Protection Act. The act established the Commission on Online Child Protection to evaluate the accessibility, cost, and effectiveness of protective technologies and methods, as well as their possible effects on privacy, First Amendment values and law enforcement. The Commission released its final report to Congress on Friday, October 20, 2000.[113]

Like the NRC commission, the COPA Commission conducted hearings, and received testimony from filtering companies, as well as filtering opponents and proponents. Among the filtering companies that testified were N2H2, ClickSafe.com, Net Nanny, Browse Safe, Cyber Patrol, Library Guardian, Exotrope, and FamilyClick.

The commissions finding on filters were summarized on page 19:

> *Server-side filtering using URL lists is available now from numerous sources.*
> *· Relative to other technologies, the best of these technologies can be highly effective in directly blocking access to global harmful to minors content on the Web and also on newsgroups, email and chat rooms. Server-side filters may be more easily implemented on a wide scale than client-side filters and may be more difficult for children to defeat.*
> *· Due to rapid growth in Internet content, server-side filters using URL lists may not be perfectly effective in blocking. Server side technologies are accessible and easy to install and require few actions by the family. Different systems offer different degrees of customizability to reflect parental values, though many offer less control than client-side systems.* [114]

Like the NRC Commission, the COPA Commission pointedly does not say that copyright protection measures are a barrier to filtering research.

**Journalists have Evaluated Filter Databases Without Research Derived from Circumventing Copyright Protection**

Commenters claim that the circumvention exemption will aid journalists in critiquing filtering software databases. Filtering software has indeed been of great interest to journalists -- a search of the Dow/Jones Factiva news database for the phrase "filtering software" during the post comment period of October 28, 2000 until February 17, 2003 retrieves 3,463 articles. Notably, commenters do not point to a single one of these 3,463 articles to support the notion that journalists will benefit from the exemption. The only example they cite is from 1996, *The Keys to the Kingdom*,[115] which is discussed on page 34.

In fact, there is a rich literature of comment and criticism about filtering software by journalists that does not involve the use of copyright circumvention techniques. Some illustrative examples since 1995 are shown below, all of which use querying methods:

In January of 2003, journalist Edward C. Baig used querying to publish an evaluation of filtering software in *USA Today*:

> *During brief tests, both CyberPatrol and Net Nanny worked adequately for the most part, although neither proved flawless. The programs let you set up different privileges for different family members, but they could be much clearer on who is being monitored at any one moment. The pair also tended to slow down my surfing a tad, even when I was headed toward legitimate online destinations.*[116]

In 2001, journalist Tom DiNome published an evaluation of filters used querying for *The New York Times*, and concluded:

> *I tried three Internet filters — Net Nanny, Cyber Patrol and We-Blocker — as well as the filtering capabilities built into the Web browsers Internet Explorer and Netscape Communicator. Each had its pros and cons, and performance varied.*[117]

In 2000, *CNET News* journalist Brian Livington used querying to publish a criticism of what he claimed was a political bias in the AOL parental controls database:

> *AOL's latest software, version 5.0, was tested by viewing more than 100 political sites over a period of several days. AOL's filters for children consistently allowed the viewing of far more conservative sites than Democratic and liberal sites. The selection remained consistent throughout the testing period.* [118]

In 1997, journalist Hope Katz Gibbs used querying to publish an evaluation of filtering software for *The Washington Post*:

> *I installed copies of four leading programs -- SurfWatch, Cyber Patrol, Cybersitter and Net Nanny -- and went trolling for smut…The results: Most programs blocked undesirable sites pretty well, but none was perfect… But parents who want some technological help in managing their kids' Internet experience should install at least one of the programs listed here.*[119]

In 1996 journalist Amy Dunkin used querying to publish an evaluation of filtering software *in Business Week*"

*This filtering function can produce curious results. All programs have enough built-in intelligence to avoid the kind of absurdity that hit America Online last year when it banned the word "breast" and cut off online discussions of breast cancer.*[120]

**Commenters Provide No Support for the "Social Benefits" of Circumventing the Copyright Protections of Filter Databases**

The commenters supporting an exemption for filtering databases provide several examples of research they claim was derived from decryptions of filter databases, and which they also claim has benefited the public. A close examination of the facts surrounding these claims reveals them to be lacking in merit.

Commenter Samuel Greenfeld asserts that:

> *Several research projects already have taken advantage of this exclusion. The results of these studies have significantly benefited the public. Ben Edelman's statistical work done for Multnomah County Public Library et al., v. United States of America, et al. demonstrated that thousands of websites may be inappropriately categorized by filtering software applications.*[121]

Mr. Greenfeld is incorrect in his assertion that "Ben Edelman's statistical work" took advantage of the filtering exclusion. This is shown in the district court ruling in the case Mr. Greenfeld cites, Multnomah v. US:

> *Benjamin Edelman, an expert witness who testified before us, compiled a list of more than 500,000 URLs and devised a program to feed them through all four filtering programs in order to compile a list of URLs that might have been erroneously blocked by one or more of the programs*[122]

As the district courts findings of fact describe, Edelman generated a sample and used the query method to conduct his research. Since Edelman's report is another example of query-based research, it undercuts, rather than supports the exemption for filtering software.

Mr. Greenfeld goes on to cite the publications of Seth Finkelstein, and Mr. Finkelstein cites two examples of his own publications, as well as a 1996 web article.[123]

The first example Mr. Finkelstein cites is decryption research he asserts he performed on behalf of the plaintiffs in the *Mainstream Loudoun* case. Finkelstein asserts that he decrypted the filtering product X-Stop, provided examples of "bad blocks" to attorneys for the plaintiffs, and finally claims that "Such evidence has played an important role in [the] litigation."[124]

Evidence from the *Mainstream Loudoun* litigation record does not support Mr. Finkelstein's claim to have been an evidence source in this case. The plaintiff's litigants, the ACLU, submitted a lengthy "Proposed Statement of Undisputed Facts", that actually describes in great detail the sources for the "bad blocks" by X-Stop submitted as evidence. Section IV, A of this document is titled "*Well Over a Hundred Sites Have So Far Been Identified by Library Staff, Patrons, Intervenors, and Others That Were Blocked Even Though They Did Not Violate The Policy and Contained Constitutionally Protected Speech*." This portion of the document describes at great length the sources of over 100 "wrongly blocked" sites submitted into evidence, and in fact credits each example to various individual "library staff, patrons, intervenors, and others" by each individual's name. Mr. Finkelstein's name appears nowhere in this document, or in any other document submitted to the Loudoun Court.[125]

But the Copyright Office need not consider the merit of Mr. Finkelstein's claim to have been an important evidence source in the *Mainstream Loudoun* case for the simple reason that the Loudoun court did not even consider this evidence in reaching its decision, as a careful reading of the Loudoun decision reveals:

> *3. Whether X-Stop Is the Least Restrictive Filtering Software*
> *Defendant claims that X-Stop is the least restrictive filtering software currently available and, therefore, the Policy [begin page 38] is narrowly tailored as applied. Our finding that the Policy is unconstitutional on its face makes this argument moot. A facially overbroad government policy may nevertheless be saved if a court is able to construe government actions under that policy narrowly along the lines of their implementation, if the policy's text or other sources of government intent demonstrate "a clear line" to draw. See Reno, 117 S. Ct. at 2350-51. we find no such clear line here. Defendant has asserted an unconditional right to filter the Internet access it provides to its patrons and there is no evidence in the record that it has applied the Policy in a less restrictive way than it is written. See Def. Resp. to Pl First Req. Admiss. 17 (denying that X-Stop does not block access to soft core pornography, which is protected). <u>Therefore, our finding that the Policy is unconstitutional on its face makes any consideration of the operation of X-Stop moot</u>. [Emphasis added]*[126]

Mr. Finkelstein next asserts that he decrypted the filtering product N2H2, and that from this decryption, he was able to make public information about an N2H2 category:

> *But I could not have exposed this secret category [N2H2 loophole], and seen that it could not ever be deactivated, as a structural, architectural, "feature" of the program, without examining the raw blacklist itself. There would be no other way of obtaining that hidden information…Here is a very concrete example - if I could not have circumvented the technological measure (encryption) controlling access to the N2H2/BESS blacklist, I would not have discovered the secret LOOPHOLE category.*[127]

Mr. Finkelstein's claim that he "could never have exposed this" without "examining the raw blacklist itself" is refuted not once, but twice by Mr. Finkelstein's own report, *Bess's Secret Loophole. Bess's Secret Loophole* actually documents two publicly available methods for gathering this information that were available at the time (August 2001) that Mr. Finkelstein wrote his report:

> *There is also a corresponding code LH which appears in log files of a N2H2 server…*
> *The LOOPHOLE category can be verified by using N2H2's single-site blacklist checking form . Just test it with an anonymizer or privacy site, e.g. http://www.safeweb.com/ , using their web form, or an equivalent URL such as http://database.n2h2.com/cgi-perl/catrpt.pl?req_URL=http://www.safeweb.com/ The result should come back as, for example:*
> *The Site: http://www.safeweb.com*
> *is categorized by N2H2 as:*
> *Loop Hole Sites.*[128]

As this passages shows, documentation of the N2H2 "Loophole" category was indeed available in August 2001 on both the N2H2 website, and by checking log files from a trial copy of N2H2's software, since these files are not encrypted and available to users.[129]

Finkelstein goes on to assert that *Bess's Secret Loophole* was "cited in expert-witness testimony for the CIPA trial, and my overall work in this area seems to have been a factor in the District Court CIPA decision."[130] A review of the ALA v U.S. decision and the trial record does not support either of these assertions.

The ALA decision indeed cites "so-called loophole sites" as one of a number of flaws in filtering software in a lengthy section titled "The Methods that Filtering Companies Use to Compile Category Lists." But at the beginning of this section the court states that "We base our understanding of these methods largely on the detailed testimony and expert report of Dr. Geoffrey Nunberg."[131]

Dr. Nunberg's expert report does indeed contain a section entitled "Loophole Sites."[132] This five-page section contains a detailed discussion of "loophole sites" and the potential problems their use in filtering can cause. But nowhere in this section or anywhere in Dr. Nunberg's report is the work of Seth Finkelstein cited.

Finally, Mr. Finkelstein cites as an example of the use of decryption research by journalists, a 1996 web-published article entitled *Keys to the Kingdom.* But an actual reading of this article raises questions about its seriousness. The author describes how he obtained a list of blocked websites while drunk in a bar:

> *I'd just spent the better part of a muggy Washington night knocking back boilermakers in an all-night Georgetown bistro waiting for a couple of NSA spooks that never showed.*
> *I tried to stumble to the door and an arm reached out and gently shoved me back to my table. At the end of that arm was a leggy redhead; she had a fast figure and even faster smile. There was a wildness about her eyes and I knew it was the crank. But something else wasn't quite right. As I fought with my booze-addled brain, struggling to focus my eyes, I noticed her adam's apple.*[133]

The probative value of *Keys to the Kingdom* was actually examined in ALA v. U.S. Plaintiff's expert Christopher Hunter submitted *Keys to the Kingdom* as evidence of the ineffectiveness of filters. During cross-examination of Mr. Hunter, the Judges expressed profound skepticism of *Keys to the Kingdom:*

> *Q: [Ms. Bhattacharyya] What the report in fact says is that the reporters were drunk in a bar in Georgetown and got the list from a transvestite, isn't that right?*
>
> *A: [Mr. Hunter] That might be the case.*
>
> *Judge Becker: Well, it says at the end, we have Brock Meeks with giving his e-mail address did the heavy drinking for this article. He Declan McCullagh giving his e-mail address did the heavy reporting. Well, at least McCullagh wasn't drunk as far as we --*
>
> *The Witness: The journalist is actually in the room but I think he's sober today.*
>
> *By Ms. Bhattacharyya:*
>
> *Q: You were aware of this article at the time you wrote you peer review masters thesis, is that right?*
>
> *A: Yes, I was.*
>
> *Q: It doesn't appear in the list of sources that you attached to your masters thesis, does it?*
>
> *A: No, it didn't.*
>
> *Judge Becker: These are all exhibits to your reports?*

*The witness: They're the supporting -- they're the full reports which I summarized in my expert*

*Judge Becker: Well, why would you summarize something like that article that Ms. Bhattacharyya just inquired about?*

*The witness: Because it provides examples of over-blocked web sites consistent in each of these reports.  Over time, all show over-blocking, under-blocking, or both.*

*Judge Fullam: But these are truly anecdotal, right?  They don't establish anything scientific very much.*[134]

## The Circumvention of Filter Database Copyright Protections has Harmed, and will Harm the Filtering Industry

As the Copyright Office already found in its 2000 *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies,* allowing the circumvention of copyright protection for databases will cause harm to the database market:

> *Finally, in assessing the effect of circumvention on the market for or value of the works, it appears likely that if circumvention were permitted, the ability of database producers to protect their investment would be seriously undermined and the market would be harmed.*[135]

This finding should certainly apply to the databases created by filtering companies as well. The harms that can be inflicted upon filtering companies are not imaginary or hypothetical.

A case exits, *Microsystems Software, Inc. v. Scandinavia Online AB*[136], that documents the harm perpetrated on a filtering company by two "researchers" -- two teen age hackers, Eddy Jansson and Matthew Skala.

The appellate court that upheld the lower court ruling in *Microsystems Software, Inc. v. Scandinavia Online AB* summarizes the litigation:

> *The plaintiffs, Microsystems Software, Inc. and Mattel, Inc. (collectively, Microsystems), developed and distributed "Cyber Patrol" -- a blocking device coveted by parents who wish to prevent their children from roaming into salacious Internet venues…shortly after Microsystems introduced Cyber Patrol, Jansson and Skala reverse-engineered it and wrote a bypass code that enabled users not only to thwart the program but also to gain access to the list of blocked sites. (1) They then posted the bypass code on their own web sites and gave blanket permission for others to copy it. The appellants took advantage of this offer…Microsystems was not pleased. On March 15, 2000, it brought suit seeking injunctive relief against the defendants and "those persons in active concert or participation with them." Microsystems complained that it was suffering irreparable injury because "[m]ultiple individuals throughout the United States and the world . . . have downloaded, copied and created 'mirror' Web sites" revealing the bypass code. When the district court issued a temporary restraining order two days later, Microsystems e-mailed copies of it, along with sundry supporting documents, to various persons (including the appellants)…Three days later, the court held a hearing on the motion for preliminary injunction. At that session, Microsystems advised the court that it had reached an accord with the named defendants and proffered a proposed final decree that purported to prohibit the defendants and those persons "in active concert" with them from posting the bypass code.*[137]

It is well worth the Copyright Office's time to review the 14-page document, *Microsystems Software, Inc. v. Scandinavia Online AB, Findings of Fact and Conclusions of Law, March 28 2000*, which is available on line at http://www.epic.org/free_speech/censorware/cp_conclusions.html. The judicial findings of fact and conclusion of law in *Microsystems* show not only the harm done to Microsystems, but provide useful insight into the motivations and methods of two such "researchers," and address the issues of "fair use" and the public good with regards to the reverse engineering of filtering software.

The *Findings of Fact* call attention to motives of the "researchers":

> *9. In their March 21, 2000 press release, Jansson and Skala admitted to "reverse engineering" the Cyber Patrol software as a means of "attack:"*
>
> > *Cyber Patrol(R) 4, a "censorware" product intended to prevent users from accessing undesirable Internet content, has been reverse engineered by youth rights activists Eddy L O Jansson and Matthew Skala… A detailed report of their findings, titled "The Breaking of Cyber Patrol(R) 4", with commentary on the reverse engineering process and cryptographic attacks against the product's authentication system, has been posted on the World Wide Web…A package of source code and binaries implementing the attacks is included.*
>
> *10. Jansson and Skala published their press release over the Internet via e-mail into the United States, including Massachusetts, and throughout the World Wide Web. Ver. Con. 17.*
>
> *11. Jansson and Skala created and promoted the Bypass Code and published it through software download links originally located on Jansson's Web page <u>to make available to children in the United States and around the world software that enables the child to defeat parents' effort s to screen inappropriate material posted on the Internet</u>. [Emphasis added] Ver. Cor. 1B.*[138]

The *Conclusions of Law* call attention to the issues of "fair use", the public good served by reverse engineering filtering software, and the adverse affects on filtering software:

> *47. The individual defendants have no "fair use" defense here because they neither asserted it nor submitted evidence supporting any fair use defense.*
>
> *48. In addition, the purpose of the copying here is inconsistent with the general public good. The individual defendents' avowed purpose for decompiling CyberPatrol was to allow "youth access" to inappropriate content on the World Wide Web. Ver. Com. 16. That purpose contradicts the public interest as specifically found by Congress:*
>
> > *The Congress finds that…while custody, care, and nurture of the child reside first with the parent, the widespread availability of computers presents opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control…the protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them is a compelling governmental interest… notwithstanding the existence of protections that limit the distribution over the World Wide Web of material that is harmful to minors, parents, educators, and industry must continue efforts to find ways to protect children from being exposed to harmful material found on the Internet.*
> >
> > *47 U.S.C. 231, The Child Online Protection Act*
>
> *49. Finally, to negate fair use one need only show that if the challenged use should become widespread, it would adversely affect the potential market for the copyrighted work. Harper & Row, Pub. Inc. V. National Ent. 417 U.S. 533. 568 (1985) (finding no fair use.)*

> *50. By their own admission, Jansson and Skala created the Bypass Code to "break" Cyber Patrol. Ver. Com., Ex. A. Software explicitly designed to make Cyber Patrol ineffective for its intended use can do nothing other than "adversely affect the potential market for the copyrighted work." Harper & Row Pub. Inc. 417 U.S. at 568.*
>
> *53. In contrast, Microsystems -- as well as the public -- will continue to suffer irreparable harm unless the individual defendants are prohibited from distributing the Bypass Code.*[139]

Notably, commenters do not even attempt to claim that any "social good" came from the efforts of Jansson and Skala. During the nearly three-year period following the publication of *The Breaking of Cyber Patrol*, commenters point to no examples of published research or journalism derived from Jansson and Skala's circumvention of Cyber Patrol's copyright protection.

In the period following the Microsystems case, it is difficult to quantify the damage to the Cyber Patrol product. The reason for this is that three months after the March 28, 2000 Microsystems ruling, the parent company of Microsystems, Mattel, Inc., sold the Cyber Patrol product to a large filtering company, SurfControl.[140] The Cyber Patrol product was then rolled in with SurfControl's other products, most of which were acquired through acquisition, including SurfWatch, Little Brother, SuperScout, and CSM.[141]

The Cyber Patrol database at the time of the acquisition was approximately 100,000[142] entries, and was rolled into several other SurfControl databases to create a new database of over 1.5 million sites.[143] The Cyber Patrol database as it was known in March 28, 2000 had ceased to exist a few months later, being absorbed into SurfControl's larger database.

But the findings of the Microsystems court make it clear that filtering companies -- and more importantly, children, will "suffer irreparable harm" by activities such as those by Jansson and Skala.

## Conclusion

This comment has documented the considerable public benefits derived from the filtering industry. Filtering software provides crucial protection for millions of children, helps to reduce liability in the workplace, increases productivity, and saves corporate bandwidth. In 1996, Congress recognized the social benefits of filtering, and passed legislation specifically designed to promote the filtering industry.[144]

This comment has also documented that there are no corresponding social benefits to allowing the circumvention of copyright control mechanisms for filtering software. The burden of proof is upon the commenters seeking an exemption to document such examples, and they have failed to meet their burden. Commenters cannot point to a single court case, ruling by a government body, or piece of independent laboratory research that benefited from such circumventions. Among the thousands of pieces of journalistic writing produced about filtering software, commenters can only point to a single example from 1996 of filtering journalism derived from copyright circumvention. The seriousness of this lone journalistic example is questionable, as it describes a reporter obtaining decryption while drunk in a bar.

This comment has provided dozens examples of laboratory research, journalism, court findings, and findings by government entities that did not require the use of research derived from circumvention. These journalists, judges, researchers, and public policy officials have drawn upon a large body of research on filtering software that uses querying methods, including research published in *Consumer Reports* and *the Journal of the American Medical Association.*

This comment has shown how circumvention of copyright controls, rather than benefiting the public, actually causes harm. This was stated best by the court in *Microsystems Software, Inc. v. Scandinavia Online AB,* which found that when a filtering company's code was reverse engineered and distributed, the filtering company, "-- as well as the public -- will continue to suffer irreparable harm unless the individual defendants are prohibited from distributing the Bypass Code."[145]

As the Copyright Office itself found when applying the DMCA to databases, "[I]n assessing the effect of circumvention on the market for or value of the works, it appears likely that if circumvention were permitted, the ability of database producers to protect their investment would be seriously undermined and the market would be harmed."[146]

For these reasons, the request for exemption for filtering databases should be denied.

FOOTNOTES

[1] 37 CFR § 201.40.

[2] 37 CFR § 201.40, 64564.

[3] 37 CFR § 201.40, 64564.

[4] 37 CFR § 201.40, 64564.

[5] Testimony of Chris Ophus, Subcommittee on Telecommunications and the Internet Hearing, "E-Rate and Filtering: a Review of the Children's Internet Protection Act," April 04, 2001. Available at http://www.house.gov/commerce/hearings/04042001-155/Ophus255.htm.

[6] 8e6 Technologies, "8e6 Database," available at http://www.8e6technologies.com/statistics/8e6categories.html.

[7] FamilyConnect, "Internet Filter," available at http://www.familyconnect.com/categories2.asp.

[8] N2H2, "Filtering Categories," available at http://www.n2h2.com/products/categories.php.

[9] Secure Computing, "Accurate URL Control List," available at http://www.securecomputing.com/index.cfm?sKey=86.

[10] SurfControl, "URL Category Database," available at http://www.surfcontrol.com/products/content/internet_databases/url_category_list/default.aspx.

[11] Websense, " The Websense Master Database: Categories," available at http://www.websense.com/products/about/database/categories.cfm.

[12] SmartFilter, " Rich feature set -- tailor your organization's Web access ," available at http://www.securecomputing.com/index.cfm?sKey=1067.

[13] 47 U.S.C. § 230 (c)(2), 110 Stat. 139 (1996).

[14] Frost & Sullivan, "Content Filtering Markets," February, 2001.

[15] Kaiser Family Foundation, "Generation Rx.com: How Young People Use the Internet for Health Information," December, 2001.

[16] Cyveillance, "Brand Names Study," March, 1999.

[17] National Center for Missing and Exploited Children, "Online Victimization: A Report on the Nation's Youth," June 2000.

[18] Digital Media Forum, Ford Foundation Survey, December 2000.

[19] Association for Supervision and Curriculum Development, "The First Amendment and Schools," May 2001.

[20] Kaiser Family Foundation, "Generation Rx.com: How Young People Use the Internet for Health Information," December, 2001.

[21] Frost & Sullivan, "Content Filtering Markets," February, 2001.

[22] The Center for Internet Studies, "Survey on Internet Misuse in the Workplace," October 1999.

[23] American Management Association, "Annual Electronic Monitoring and Surveillance Survey," 2001.

[24] Time Magazine, "On a Screen Near You: Cyberporn," July 3, 1995.

[25] Business Wire, "Solid Oak Software Inc. has announced the release of its latest product, CYBERsitter," June 26, 1995.

[26] PR Newswire, "Microsystems Software Announces Cyber Patrol(TM) Internet Access Management Utility; Cyber Patrol lets parents and teachers control children's access to the Internet," July 31, 1995.

[27] Business Wire, "SurfWatch blocks Internet pornography, breakthrough product ships today" May 15, 1995.

[28] Reno v ACLU, 521 U.S. 844 (1997).

[29] National Center for Education Studies, "Internet Access in U.S. Public Schools and Classrooms: 1994 – 2000," May 2001.

[30] Library Journal, "Annual Public Library Budget Survey," Jan. 15, 2002.

[31] American Management Association, "Annual Electronic Monitoring and Surveillance Survey," 2001.

[32] Pew Foundation, "Internet and American Life Project," June 2001.

[33] IDC, "Worldwide Secure Content Management Software Market Forecast and Analysis, 2002–2006: Vendor Views," June 2002. Analysts: Brian Burke, Christian A. Christiansen, and Charles Kolodgy.

[34] Quality Education Data, "Internet Usage in Public Schools 1998, 3rd Edition", 1998.

[35] Quality Education Data, "Internet Usage in Public Schools 1999, 4th Edition", 1999.

[36] National Center for Education Studies, "Internet Access in U.S. Public Schools and Classrooms: 1994 – 2000," May 2001.

[37] American Management Association, "Annual Electronic Monitoring and Surveillance Survey," 2000.

[38] American Management Association, "Annual Electronic Monitoring and Surveillance Survey," 2001.

[39] Family PC, "Net parent survey," December 1997.

[40] National Center for Missing and Exploited Children, "Online Victimization: A Report on the Nation's Youth," June 2000.

[41] Pew Foundation, "Internet and American Life Project," June 2001.

[42] National Commission on Libraries and Information Science, "Public Libraries and the Internet 1998", 1998.

[43] National Commission on Libraries and Information Science, "Public Libraries and the Internet 2000", 2000.

[44] Library Journal, "Annual Public Library Budget Survey," Jan. 15, 2002.

[45] 37 CFR § 201.40, 64566.

[46] LexisNexis, "GENERAL TERMS AND CONDITIONS FOR USE OF THE LEXISNEXIS™ SERVICES. Effective April 1, 1996." Available at http://www.lexisnexis.com/terms/general/.

[47] Dialog, "Profound Subscription and Single Site License Agreement." Available at http://support.dialog.com/terms/profound.shtml.

[48] Burt, David, "Comments of N2H2 to the NTIA," August 2001. Available at http://www.ntia.doc.gov/ntiahome/ntiageneral/cipacomments/comments/n2h2/N2H2.htm.

[49] SurfControl, "URL Category Database," available at http://www.surfcontrol.com/products/content/internet_databases/url_category_list/default.aspx.

[50] 8e6 Technologies, "8e6 Database FAQ," http://www.8e6technologies.com/statistics/8e6faqs.html.

[51] SC Magazine, "Five-Star Review of Websense Enterprise," January 2002. Available at http://www.websense.com/company/news/companynews/02/010102c.cfm.

[52] Websense, "The Websense Master Database, " Available at http://www.websense.com/products/about/database/index.cfm.

[53] Net Nanny, "Net Nanny 5.0 User Guide," page 23. Available at http://www.netnanny.com/products/netnanny5/docs/NN5USRG.pdf.

[54] London Telegraph "Burger King gives away porn addresses," June 22, 2000.

[55] Seattle Post-Intelligencer, "Besieged Net Nanny will file for protection," June 11, 2002.

[56] Websense, "Why Quality Matters." Available at http://www.websense.com/whyqualitymatters/index.cfm.

[57] N2H2, " Department of Justice Study Finds N2H2 Internet Filtering to be Most Effective," April 9, 2002. Available at http://www.n2h2.com/about/press/releases.php.

[58] N2H2, "Internet Filtering Scores Major Victory in Kaiser Family Foundation Study," December 11, 2002. Available at http://www.n2h2.com/about/press/releases.php.

[59] Washington Post, "Putting Up Walls on the Web; America Online and MSN Roll Out Child-Protection Controls," November 12, 2002.

[60] 37 CFR § 201.40, 64567.

[61] London Telegraph "Burger King gives away porn addresses," June 22, 2000.

[62] PR Newswire, "SurfControl's Most Advanced Internet Safety and Access Management Software Ready for Back to School," August 8, 2001.

[63] N2H2 "Product evaluations," available at http://www.n2h2.com/downloads/eval.php; Websense "Trial Software," available at http://www.websense.com/downloads/index.cfm; SurfControl, "Download center," available at http://www.surfcontrol.com/downloads/Default.aspx; etc.

[64] Boyce, Bert R., "Measurement in information science," Chapter 10, "Measurement of Databases," page 149-150. Academic Press, 1994.

[65] Boyce, Bert R., "Measurement in information science," Chapter 13, "Measurement of Retrieval Outcome," pages 176-193. Academic Press, 1994.

[66] Boyce, Bert R., "Measurement in information science," Chapter 13, "Measurement of Retrieval Outcome," page 176. Academic Press, 1994.

[67] Paris, Lee Anne H.; Tibbo, Helen R, "Freestyle Vs. Boolean: A Comparison of Partial and Exact Match Retrieval Systems," Information Processing & Management; v34 n2-3 p175-90 Mar-May 1998.

[68] Diamond, Rand J., "Comparing Lexis and Westlaw: Using System Features To Improve Search Results," Kent State University, 1991.

[69] Hood, William W. & Wilson, Concepcion S, "The Scatter of Documents over Databases in Different Subject Domains: How Many Databases Are Needed?," Journal of the American Society for Information Science and Technology; v52 n14 p1242-54 Dec 2001.

[70] Pritchard-Schoch, Teresa, "Comparing Natural Language Retrieval: WIN and FREESTYLE," Online; v19 n4 p83-87 Jul-Aug 1995.

[71] Gillaspie, Deborah L., "Why Online Legal Retrieval Misses Conceptually Relevant Documents," Proceedings of the ASIS Annual Meeting; v29 p256-59 1992.

[72] Dennis, Simon; Bruza, Peter; McArthur, Robert, "Web Searching: A Process-Oriented Experimental Study of Three Interactive Search Paradigms," Journal of the American Society for Information Science and Technology; v53 n2 p120-33 Jan 15, 2002.

[73] Caroline R. Richardson, MD; Paul J. Resnick, PhD; Derek L. Hansen, BS; Holly A. Derry, MPH; Victoria J. Rideout, MA, "Does Pornography-Blocking Software Block Access to Health Information on the Internet?," JAMA. 2002;288:2887-2894.

[74] Consumer Reports, "Is your kid caught up in the Web?," May 1997.

[75] Consumer Reports, "Digital chaperones for kids," March, 2001.

[76] ZDNet, "About ZDNet Labs," 2002. Available at http://www.zdnet.com/products/stories/reviews/0,4161,2761376,00.html.

[77] PC Magazine, "Monitor a Child's Access," March 24, 1998.

[78] PC Magazine, "Corporate Monitoring/Filtering: Make Net Work, Not Play," May 4, 1999.

[79] PC Magazine, "Clean it Up," September 25, 2001.

[80] InfoWorld Website, "About InfoWorld." Available: http://www.infoworld.com/aboutus/t_about_infoworld.html.

[81] InfoWorld, "About the Test Center," http://www.infoworld.com/tc/t_about.html.

[82] InfoWorld, "WebSense sets up a flexible line of defense for screening Web sites," August 18, 1997.

[83] InfoWorld, "Cyber Sentinel 1.4 adds intelligence capabilities," February 16, 1998.

[84] PC World, "The Smut Stops Here or Does it?" October 1997.

[85] Internet Magazine, "Policing the Net," December 1997.

[86] Network World site, "Network World Test Alliance." Available: http://www.nwfusion.com/alliance/index.html.

[87] Network World, "Where do you think you're going?," October 5, 1998.

[88] Network Computing, "Regulating Web Surfing," February 7, 2000.

[89] EWeek, "SmartFilter 3.0 plug-in corrals Net use," February 19, 2001.

[90] Internet World, "Safe computing," September 1996.

[91] E-Testing Labs, "U.S. Department of Justice: Filtering Software Comparison," Oct. 2001. Available at http://www.etestinglabs.com/clients/reports/usdoj/usdoj.pdf.

[92] E-Testing Labs, "Corporate Content Filtering Performance and Effectiveness Testing," April 2002. Available at http://www.websense.com/whyqualitymatters/etestinglabs-fullreport.pdf.

[93] CERTUS Consulting Group, "Internet Filtering Accuracy Review," October 15, 2001.

[94] Biek, David. "Evaluation of Cyber Patrol Logs", January 2000.

[95] American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996), aff'd, 521 U.S. 844 (1997).

[96] A full transcript of Ms. Duvall's testimony is available at http://www.epic.org/free_speech/cda/lawsuit/transcript_3_21.2.html.

[97] American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996), aff'd, 521 U.S. 844 (1997).

[98] American Civil Liberties Union v. Reno, 31 F. Supp. 2d 473 (1999), aff'd, 217 F.3d 162 (3d Cir. 2000).

[99] American Civil Liberties Union v. Reno, 31 F. Supp. 2d 473 (1999), aff'd, 217 F.3d 162 (3d Cir. 2000).

[100] American Library Ass'n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002).

[101] American Library Ass'n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002)
Nunberg Test. (3/26/02), at 84.

[102] American Library Ass'n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002) Edelman Test. (4/2/02), at 101.

[103] American Library Ass'n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002) Hunter Test. (3/26/02), at 219-20.

[104] American Library Ass'n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002) Defts' Ex. 184 (eTesting Labs Report. Report available at http://www.etestinglabs.com/clients/reports/usdoj/usdoj.pdf.

[105] American Library Ass’n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002), Defts' Ex. 179 (Finnell Expert Report).

[106] American Library Ass’n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002), Biek Test. (3/28/02), at 79.

[107] American Library Ass’n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002).

[108] American Library Ass’n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002).

[109] American Library Ass’n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002).

[110] Mainstream Loudoun v. Board of Trustees of the Loudoun County Library, 24 F. Supp. 2d 552, 563 (E.D. Va. 1998).

[111] "Youth, Pornography, and the Internet", National Research Council, page 10.

[112] "Youth, Pornography, and the Internet", National Research Council, Box 2.7.

[113] Commission on Child Online Protection (COPA) Report to Congress, October 20, 2000, available at http://www.copacommission.org/report/COPAreport.pdf.

[114] Commission on Child Online Protection (COPA) Report to Congress, October 20, 2000, at 19, available at http://www.copacommission.org/report/COPAreport.pdf.

[115] C 33 Seth Finkelstein.

[116] Baig, Edward C., "Keeping Internet predators at bay," USA Today, January 29, 2003. Available at http://www.usatoday.com/tech/columnist/edwardbaig/2003-01-29-baig-safety_x.htm.

[117] DiNome, Tom, "Filtering the Web for Young Users," The New York Times, September 27, 2001.

[118] AOL's "youth filters" protect kids from Democrats, By Brian Livingston April 24, 2000. Available at http://news.com.com/2010-1080-281304.html.

[119] Katz Gibbs, Hope, " Porn-Free; Software to Block the Hardcore," The Washington Post
April 25, 1997.

[120] Amy Dunkin, "CyberSmut: How to Lock out the kids," Business Week, Feb. 12, 1996.

[121] C32 Samuel Greenfeld.

[122] American Library Ass’n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002).

[123] C33 Seth Finkelstein.

[124] C33 Seth Finkelstein.

[125] ACLU, "Proposed Statement of Undisputed Facts," September 4, 1998. Available at http://archive.aclu.org/court/loudoun_facts.html.

[126] Mainstream Loudoun v. Board of Trustees of the Loudoun County Library, 24 F. Supp. 2d 552, 563 (E.D. Va. 1998).

[127] C33 Seth Finkelstein.

[128] Seth Finkelstein, "Bess's Secret Loophole," August 2001. Available at http://www.sethf.com/anticensorware/bess/loophole.php.

[129] The N2H2 Technical Support website states that " The filter_log file contains the URL requests in raw format" on the page "Support for Bess Internet Filtering," available at http://www.n2h2.com/support/bess.php?device_type=lnx&content=faq.

[130] C33 Seth Finkelstein.

[131] American Library Ass’n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002).

[132] American Library Ass’n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002), (Nunberg Expert Report).

[133] Meeks, Brock and McCullagh, Declan, "The Keys to the Kingdom," CyberWire Dispatch, July, 1996. Available at http://www.eff.org/Publications/Declan_McCullagh/cwd.keys.to.the.kingdom.0796.article.

[134] American Library Ass'n v. Aschroft, Civil Action No, 01-1303 (E.D. Pa.), Trial Tr., Hunter Test. (3/26/02), at 219-20.

[135] 37 CFR § 201.40, 64567.

[136] Microsystems Software, Inc. v. Scandinavia Online AB, 98 F. Supp. 2d 74 (D. Mass. 2000).

[137] Microsystems Software, Inc. v. Scandinavia Online, 226 F.3d 35 (1st Cir. 2000).

[138] Microsystems Software, Inc. v. Scandinavia Online AB, 98 F. Supp. 2d 74 (D. Mass. 2000), Findings of Fact and Conclusions of Law.

[139] Microsystems Software, Inc. v. Scandinavia Online AB, 98 F. Supp. 2d 74 (D. Mass. 2000), Findings of Fact and Conclusions of Law.

[140] Business Wire, "JSB Software Technologies plc Announces Agreement With Mattel, Inc. to Acquire Cyber Patrol For US$100m," June 26, 2000.

[141] The Independent - London , "Corporate Profile - Big Brother is watching you," September 13, 2000.

[142] CNN, "Cyber Patrol decoding brawl gets ugly and international,"March 21, 2000. Available at http://www.cnn.com/2000/TECH/computing/03/21/cyberpatrol.decoder/.
[143] M2 Presswire, "Surfcontrol solidifies no. 1 market position in Internet management software," October 25, 2000.
[144] 47 U.S.C. § 230 (c)(2), 110 Stat. 139 (1996).
[145] Microsystems Software, Inc. v. Scandinavia Online AB, 98 F. Supp. 2d 74 (D. Mass. 2000), Findings of Fact and Conclusions of Law.
[146] 37 CFR § 201.40, 64567.