

## Who Defines Evil?

### Statement Regarding the Kaiser Family Foundation Study on How Filtering Affects Access to Health Information

Nancy Willard, M.S., J.D.

Director, Center for Safe and Responsible Internet Use (was Responsible Netizen Institute)

P.O. Box 50412, Eugene, Oregon 97405

URL: <http://saferesponsibleinternet.org>

E-Mail: [nwillard@saferesponsibleinternet.org](mailto:nwillard@saferesponsibleinternet.org)

(541) 344-9125

December 2002

On December 10th, 2002, the Kaiser Family Foundation issued a new study, *See No Evil: How Internet Filters Affect the Search for Online Information*. This study is available on their site at <http://www.kff.org/content/2002/20021210a/>.

Kaiser researchers studied the issue of youth access to health information when filtering software has been installed. Kaiser studied the six leading filtering products that are used in U.S. public schools, SmartFilter, 8e6, Websense, CyberPatrol, Symantec, and N2H2, along with AOL Parental Controls.

They assessed the ability to access sites containing health information across a broad range of topics, including health topics unrelated to sex, health topics that relate to sexual body parts, health topics related to sex, and sites presenting potentially controversial health information

The six filters used in public schools were set at three different configurations: least restrictive -- blocking only the pornography-related category or categories; intermediate restrictive -- blocking those categories that are most likely to be considered inappropriate; and most restrictive -- blocking all categories conceivable in a library or school setting. Most public schools have configured their filtering systems at or above the intermediate restrictive configuration.

Kaiser researchers also tested the systems ability to block access to pornography under conditions simulating intentional access and accidental access. To assess accidental access, they attempted to access the pornography sites that appeared in the search results when they were seeking appropriate health information.

#### **Highlights of the Study.**

Under conditions simulating intentional access, one in ten (1 in 10) sites containing pornography were accessible. This failure rate was consistent across the blocking configurations. (Least -- 87%; Intermediate -- 90%; Most -- 91%) Consider how long it would take a student or staff member at an unsupervised computer to test ten pornography sites to find the one unblocked site. If schools do not have effective supervision and engage in regular review of blocked URL reports, such intentional attempted access would go undetected. U.S. public schools are spending billions of dollars for approximately 2 minutes of protection.

Under conditions simulating accidental access, the filters allowed access to pornography 38% of the times -- one in three (1 in 3) times. Educators and parents who think that filters will protect Suzie from accidentally accessing pornography when she is searching for information on kitties should think again.

Kaiser found across all of the health information that filters set at the least restrictive level blocked only 1.4% of the health information sites. They blocked only 5% of such sites at the intermediate level. However, filters blocked 24% of such sites at the most restrictive level.

A closer analysis of the data reveals blocking patterns that present significantly greater concerns. In those categories where the subject area is controversial or the sites themselves may contain controversial information, the rate of overblocking was significantly higher. The categories that stood out included safe sex, homosexuality, and drugs. At the intermediate restriction configuration, typical of most school settings, the filters blocked one in four (1 in 4) of the health information sites in these subject areas.

The Kaiser study demonstrates the reasons why it is both unwise and inappropriate to place reliance on filtering software to protect young people when they are using the Internet.

### **The Danger of False Security and Complacency**

Filtering companies and their conservative pro-filtering allies promise that filtering will protect young people on the Internet. This misrepresentation creates a dangerous level of false security and complacency. It is dangerous to believe that we can protect young people by establishing electronically fenced playpens. The snakes can still get in and teens can easily get out.

Filtering software is not infallible, it does not protect against all concerns and it is not, and will never be, present on all computers that our young people will access. Filters are not the solution. They will never be the solution.

This study clearly demonstrates the concerns about placing reliance on filtering software. In conditions simulating intentional access, the filters failed to work 10% of the time -- one out of ten (1 in 10) sites. Consider how long it would take a curious teen or a staff member at an unsupervised computer to check out ten blocked sites to find the one that is unblocked.

Many educators think that filters are protecting students and therefore it is acceptable to allow unsupervised use. In many schools, the blocked URL reports are not reviewed on a regular basis. Under such circumstances, it would not take long for students or staff members to determine that intentional attempts to access pornography will go undetected and unpunished. U.S. public schools are spending billions of dollars for approximately two minutes of protection.

Even more concerning is the data resulting from conditions simulating inadvertent access. Under these conditions, the filter failed to block access 38% of the time. Filtering companies want us to believe that by installing filters we will protect Suzie while she is innocently searching for information on kitties. Assuming this data is correct, one out of three (1 in 3) Suzie makes a mistake she will end up at a pornography site.

If Suzie is a young child, then we simply must do a better job of protecting Suzie by keeping her in places that are truly safe and by closely supervising all Internet use. As Suzie approaches her teen years, it is time to teach Suzie how to avoid accidentally accessing the wrong kinds of sites, what to do if she has gotten to a wrong site especially if she has been ensnared, how to recognize and deal with harassers, perverts, and predators, and her responsibilities as a cybercitizen.

When people believe in the false promises of the filtering companies, they frequently fail to engage in the education and supervision necessary to truly protect young people on the Internet. Case in point -- the Children's Internet Protection Act contains extensive requirements related to the use of technology protection measures -- but it does not mention Internet safety education even once.

How many school districts are relying on filtering software, but not teaching students about safe and responsible use?

### **Blocking of Sites Containing Controversial Information or Related to Controversial Subjects**

The Kaiser study also demonstrates why it is inappropriate, under First Amendment standards of access to information, for filtering to be used in schools.

The leading case in this area is the case of *Pico v. Island Trees Board of Education*. In this case school board members received a list of "objectionable books" from a conservative parent organization and sought to remove those books from their school library. The leading decision stated the constitutional standard clearly, "School boards may not remove books from school libraries simply because they dislike the ideas contained in those books."

What the Kaiser study has very effectively demonstrated is intentional or inadvertent blocking of potentially controversial information or information related to controversial subjects.

At the configuration most likely to be considered necessary to protect students from inappropriate material on the Internet -- the intermediate restriction configuration -- filters are blocking approximately one of every four (1 in 4) sites in areas where there is the potential of controversy. This is so even though those blocked sites were identified by the researchers as containing health information. This pattern is evident in the controversial sexual-related categories of "safe sex," "condoms," "gay," and "lesbian."

The pattern is also evident in the category addressing the illicit drug "ecstasy." The illegal drug filtering categories were not blocked at the least restrictive configuration but were at the intermediate configuration. One in four (1 in 4) health sites addressing ecstasy were blocked at the intermediate configuration.

#### **Health Information Sites Blocked (%)**

Category	Least	Intermediate	Most
All health sites	1.4	5	24
Ecstasy	0.3	24.9	36.2
Safe sex	9.3	20.5	50.0
Condoms	9.1	27.7	55.4
Gay	11.1	24.6	59.9
Lesbian	3.8	24.6	59.0

This pattern of intentional or accidental blocking of potentially controversial information is highly concerning. Consider what other issues might also be subject to this pattern, including, most specifically, sites that present politically controversial information. These sites could easily be blocked in some of the categories selected at the intermediate configuration level, such as intolerance, anarchy, or extremist.

### **Far Removed from Accountability**

The Kaiser Family Foundation did not address the issue of lack of public accountability directly. But the fact that the foundation found it necessary to conduct this study raises concerns about the overall lack of public information pertaining to how filtering decisions are made.

What the dissent in the *Pico* said was also instructive with respect to the use of filtering by public institutions. The dissent said:

We can all agree that as a matter of educational policy students should have wide access to information and ideas. But the people elect school boards, who in turn select administrators, who select teachers and these are the individuals best able to determine the substance of that policy. ... A school board is not a giant bureaucracy far removed from accountability for its actions.

When school officials implement the use of filtering, they have abdicated control over what materials students may or may not access to private companies that are far removed from accountability for their actions. The illusory level of control that can be exercised at the local level is the selection of categories -- a selection based on a one sentence description of what is blocked in that category, with some examples but without an accurate description of the criteria for blocking within the category.

Beyond the one sentence description, the filtering companies protect all further information about how and what they are blocking as confidential trade secret information. This includes all blocking criteria, key words that are used to identify the sites, information about the decision-making process, and the blocked list itself. Little to no information is available about the executives or investors whose interests and values may be influencing the blocking criteria and decision-making. Most of these companies are also serving or pursuing a variety of customers -- including conservative religious Internet service providers and repressive third world countries -- whose interests may be impacting the blocking criteria and decision-making

There is absolutely no public disclosure. Therefore, these companies are far removed from accountability for their actions. There is also now strong evidence of significant intentional or accidental blocking of sites that present controversial information or address controversial subjects. We have no knowledge on how or why this overblocking is occurring.

The filtering companies will suggest that the ability to override the filter provides the necessary local control. If the companies were merely making a few mistakes in their blocking, this might be a reasonable cure. But these companies are engaging in significant overblocking of potentially controversial information.

When a site is blocked, the user has no insight as to whether this is a good or bad site, so there is a reluctance to request for an override, especially if the subject matter is controversial. The override process is generally untimely and too burdensome. Students desiring access to potentially controversial information are reluctant to request that the filter be overridden. Overriding is simply not an adequate cure.

Under these conditions, how can it be considered constitutional for these products to be used in public institutions?

### **Comprehensive Education and Supervision Approach**

To truly protect young people on the Internet, we need to embrace a comprehensive approach that keeps younger children in very safe places, and that provides older children with education and continued adult involvement to impart the knowledge, skills, motivation, and values to use the Internet in a safe and responsible manner.

In schools, this can be done within the context of the Children's Internet Protection Act, by using alternative technologies, such as those described in the National Research Council's new study, *Youth, Pornography and the Internet*.

While there is a role for technologies to play in protection and monitoring, we cannot continue to rely on technological quick fixes as surrogates for the more important responsibilities of education and continued adult involvement. We simply must focus our efforts on helping young people develop effective filtering and blocking systems that will reside in the hardware that sits upon their shoulders.

### **About the Author**

Nancy Willard, M.S., J.D. is a recognized authority on issues related to the safe and responsible use of the Internet by young people and legal and policy issues related to the use of the Internet in public schools. She testified before the Children's Online Protection Act Commission and the National Research Council committee studying Internet pornography on educational strategies to address the concerns of youth access to sexually explicit material. She is the author of *Computer Ethics, Etiquette, and Safety for the 21st Century Student*, published by the International Society for Technology in Education. Her new book, *Safe and Responsible Use of the Internet: A Guide for Educators*, provides guidance for school districts on comprehensive approaches to address the concerns of student use of the Internet. This book is available through the Responsible Netizen Institute web site <http://responsiblenetizen.org/srui.html>.