

Why Filters are Not the Answer¹

In 1998, Congress passed the Child Online Protection Act (COPA), which required age verification screens for websites containing material “harmful to minors. COPA was an attempt to remedy the defects that the Supreme Court found in the Communications Decency Act (CDA). With COPA, Congress “created what it believed was a statute that would protect children from exposure to obscene professional photography without obstructing adult access to material that the First Amendment protects.”² However, the Supreme Court subjected COPA to strict scrutiny and found that the Government did not meet its burden of proof in showing that less restrictive alternatives (especially filters) would be less effective.³ Justice Breyer, joined by Chief Justice Rehnquist and Justice O’Connor, dissented, arguing that Internet filtering software, “as presently available, does not solve the ‘child protection’ problem” because it suffers from “serious inadequacies that prompted Congress to pass legislation instead of relying on its voluntary use.”⁴

Filters have until now been the best choice for blocking pornographic Internet content. Thus, most anti-pornography groups have enthusiastically promoted the use of filters. Certainly, although filters are expensive and deplete computer efficiency, filters are better than nothing; they block sites that use any of a list of sexual terms and other signals of inappropriate material that the technology can be programmed to detect. But the best filters, relying as they must on technology rather than human review of every site, miss things, especially images without text and misspelled or disguised terms. Further, pornographers are developing technology for evading filters as fast or faster than filter companies can upgrade filters. Finally, and most importantly, anyone with technological skills (or who has a friend with technological skills or access to a chat room) can get past a filter. One hundred percent of the many teenagers interviewed at random by CP80 volunteers could easily explain how to circumvent the most sophisticated filters. They described filters as less than a bump in the road to accessing the most potent forms of obscenity. Yet, parents and schools and employers bask in a false sense of security because they believe their filter is doing the job. Even more disturbing, the Supreme Court is using the existence of filtering devices as an excuse to strike down the attempts of Congress to do something to protect our children from Internet pornography. Thus, although marginally helpful, filters have become part of the problem.

This paper will discuss five reasons why filters are inadequate to protect against Internet pornography. First, filters are under-inclusive; they do not identify and block all inappropriate or obscene content. Second, filters erroneously block a great deal of useful Internet content that is not harmful to children. Third, filters are easily circumvented. Fourth, filters cost money and require installation and maintenance. Because they are simply optional, filters are underused. Fifth, filters drain computer processing efficiency, making computers slower and limiting the range of functions they can perform. Because of these reasons, neither parents nor the government should “rely exclusively on [filtering] technology to protect ... children,”⁵ for, “despite the availability of filtering software, children [are] still being exposed to harmful material on the Internet.”⁶

1. Under-Inclusion

The first reason why Internet filters are an inadequate and unreliable is that no filtering technology is yet capable of blocking all undesirable sites. A Kaiser Family Foundation study found that, at their most restrictive settings, Internet filters were unable to block about ten percent of pornographic websites.⁷ An unrelated, but earlier, study conducted by Christopher Hunter found that filters failed to block objectionable content (which included violence, pornography, and language) 25% of the time.⁸ It is estimated that approximately 372 million pornographic web pages exist.⁹ This means that, if all parents, schools, libraries, and other internet-enabled computer providers utilized Internet filters on their most restrictive settings, children would still be exposed to and unprotected from at least 37 million pornographic web pages, and possibly as many as 90-100 million.¹⁰

The gaps in filter protection occur for various reasons. Filtering systems that rely on established lists of pornography sites to filter out indecent websites quickly become outdated.¹¹ Filtering systems that analyze the text on websites fail to block sites that “consist mainly of indecent images without text.”¹² Also, “Web site publishers can...use image files to place words on the screen that a filter cannot ‘see.’”¹³ Further,

Accurate filter operation is also increasingly frustrated with clever tricks used by the Internet's pornography promoters. Words that may be in a filter's dictionary of target keywords can be written in code or simply altered to fool automated filtering. . . . There is currently no technology protection measure that can effectively protect against access to harmful visual depictions.¹⁴

Because Internet pornographers are currently “using creative techniques to get around ... filtering software,”¹⁵ children are still at risk when online.

2. Over-Inclusion

Because many filters are based on textual analysis, they block many useful websites that are not pornographic. “Filters generally cannot construe the context of the supposed objectionable term or phrase,” and will therefore “deny access to innocuous web pages.”¹⁶ An obvious example is a filter that uses textual analysis set to block pornographic websites using the word “breast.” It would also deny access to web pages with information on “women and cancer (“breast” cancer), neonatal health (“breast” feeding), and chicken recipes (chicken “breast”).¹⁷ Similarly, a block on the word “sex” blocks sites that have data on gender studies, dog breeding, and color blindness. Christopher Hunter's study also found that filters “improperly blocked 21% of benign content.”¹⁸ Furthermore, “overinclusive filters cause particular damage to any content dealing with gays, safe sex material, and left-leaning political groups.”¹⁹

In an attempt to address the notorious problem of under-inclusion, “some filter manufacturers make sure that their filters preference over-inclusion.”²⁰ The National Research Council found that “[b]ecause most filters are deployed to forestall complaints, and most complaints are more likely to be received about underblocking rather than overblocking, filter vendors have more incentive to block content that may be controversial than to be careful about not blocking content that should not be blocked.”²¹ The report cited two other reasons for overblocking. First, filters cannot keep up with

changes on web pages. A site that may have been blocked for good reason in the past may “post new information” that is “completely innocuous.”²² Second, if a site contains both appropriate and inappropriate material and the filter is incapable of separating the material, it will usually block the entire site or web page.²³

Another threat is described by Lawrence Lessig, a prominent scholar in free speech jurisprudence:

There is a lot of good evidence about how poorly this technology filters cyberspace: how it filters the wrong type of material. There are also more insidious examples of what the companies that release this software do. For example, if you become known as a critic of that software, mysteriously your Web site may appear on the list of blocked Web sites, which becomes an extraordinary blacklist of banned books. The problem with this blacklist of banned books is that the public cannot look at it.²⁴

As Justice Breyer stated, a “[filter] blocks a great deal of material that is valuable.”²⁵

3. Easy Circumvention

“[T]he high level of computer literacy of children allows them to bypass filters through tricks that go undetected by their less computer savvy parents.”²⁶ The National Research Council identified various ways in which children can get around filtering software.²⁷ For example, youth can uninstall the filter, disable the filter (in many homes, the “resident teenager serves as the de facto system administrator because of superior technical knowledge”), access the web page indirectly through a proxy, find a different click route to the page, and “manipulate the reload/refresh and back/forward keys.”²⁸

In addition, “inappropriate material ... can flow to a child through routes other than web sites—peer-to-peer file transfers, e-mail attachments, and so on.”²⁹ The ICPSA makes posting such material onto Community Ports illegal, and will be an important weapon even in protecting kids from each other.

4. Cost, Complexity and the Underuse of Filters

Justice Breyer stated that “[f]iltering software costs money.”³⁰ Although “[f]ilters are perhaps the most widely deployed of all technological tools intended to protect children from exposure to inappropriate material,” they are severely underused.³¹ About one in four families that have Internet access use some form of parental controls (either store-bought or ISP-provided filtering software).³² This means that, “as a percentage of all children using the Internet, the fraction whose Internet access is filtered apart from school usage is small.”³³ The “existence and the benefits of filters remain unknown to many parents,”³⁴ and, for a variety of other reasons, “including cost of blocking technology and parental ... naïveté and indifference, many parents don’t use screening technology.”³⁵

Conclusion

The proof is in the pudding. Internet filters have been available for many years. Children are still accessing pornography on the Internet. For example, a 1999 TIME/CNN teen poll found that 44% of teens between 13-17 years old had seen “websites that are X-rated or have sexual content.”³⁶ An Australian study in 2003 found

that 84% of boys and 60% of girls ages 16-17 had accidentally entered pornographic web sites.³⁷ Even worse, 38 % of the boys admitted to having “deliberately searched the Internet for pornography.”³⁸ These figures are sobering, but in the years since these studies were conducted, the access of underage Internet users has skyrocketed. Recent studies report that roughly 78% of America’s youth ages 2-17 have access to the Internet.³⁹

Relying on filters has become dangerous. Filters lure us (and more importantly the Supreme Court) into thinking the problem with Internet pornography is under control. Talk to teenagers who will be honest with you (probably not your own kid), and you will discover a generation drowning in vivid images of behavior many of us would find unimaginable. Internet use begins young; as soon as a child enters puberty (or thinks he or she should be interested in such matters), curiosity and peer pressure drive them to see what their friends are seeing and, ultimately to prove they “fit in,” to do what their friends learned to do on the Internet. They have moved far past what parents believe their filters block.

Footnotes:

1. Cheryl B. Preston, Edwin M. Thomas Professor of Law. I note that a very recently issued opinion on COPA provided findings of fact and law on the issue of filters. *See* *ACLU v. Gonzales*, 478 F.Supp.2d 775 (2007). This paper does not directly address the claims raised in that case about the effectiveness of filters. That is the subject matter of another paper, currently in progress.
2. *Ashcroft v. ACLU [Ashcroft III]*, 542 U.S. 656, 690 (2004) (Breyer, J., dissenting).
3. *See id.* at 667-68.
4. *Id.* at 684-85.
5. Susan Hanley Kosse, *Try, Try Again: Will Congress ever get It Right?* 38 U. RICH. L. REV. 721, 775 (2004).
6. William H. Jordan, *Protecting Speech v. Protecting Children: An Examination of the Judicial Refusal to Allow Legislative Action in the Realm of Minors and Internet Pornography* 57 S. C. L. REV. 489, 501 (2006).
7. *See* HENRY J. KAISER FAMILY FOUNDATION, *SEE NO EVIL: HOW INTERNET FILTERS AFFECT THE SEARCH FOR ONLINE HEALTH INFORMATION, EXECUTIVE REPORT* (2002), <http://www.kff.org/entmedia/upload/See-No-Evil-How-Internet-Filters-Affect-the-Search-for-Online-Health-Information-Executive-Summary.pdf>.
8. *See* Christopher D. Hunter, *Internet Filter Effectiveness—Testing Over- and Under-Inclusive Blocking Decisions of Four Popular Web Filters*, 18 SOC. SCI. COMP. REV. 214, 220 (2000).
9. *See* Jordan, *supra* note 5, at 489.
10. The Kaiser Family Foundation study painted the ninety percent success rate in blocking pornography as a success. However, critics of this viewpoint see it as a major failure. For example, “the filters failed to work (ten percent) of the time – one out of ten (1 in 10) sites. Consider how long it would take a curious teen...to check out ten blocked sites to find the one that is unblocked.” NANCY WILLARD, WHO DEFINES EVIL: STATEMENT REGARDING THE KAISER FAMILY FOUNDATION STUDY ON HOW FILTERING AFFECTS ACCESS TO HEALTH INFORMATION (2002), <http://csriu.org/onlinedocs/pdf/whodefinesevil.pdf>.
11. *See* Steven E. Merlis, *Preserving Internet Expression while Protecting our Children: Solutions Following Ashcroft v. ACLU*, 4 NW. J. TECH & INTEL. PROP. 117, 127 (2005).
12. *Id.*; *see also* *U.S. v. American Library Ass’n, Inc.*, 539 U.S. 194, 221-22 (Stevens, J., dissenting) (acknowledging that, because of the lack of image recognition technology, a substantial amount of pornographic/obscene Internet material will remain unblocked).

13. Jared Chrislip, *Filtering the Internet like a Smokestack: How the Children's Internet Protection Act Suggests a New Internet Regulation Theory*, 5 J. HIGH TECH. L. 261, 272 (2005).
 14. *Id.*
 15. Jacob A. Sosnay, *Regulating Minors' Access to Pornography via the Internet: What Options does Congress Have Left?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 453, 480 (2005).
 16. Chrislip, *supra* note 12, at 271.
 17. *See id.*
 18. Hunter, *supra* note 7, at 220.
 19. *Id.* at 221.
 20. Merlis, *supra* note 10, at 128.
 21. DICK THORNBURG, NATIONAL RESEARCH COUNCIL, YOUTH, PORNOGRAPHY, AND THE INTERNET § 12.1.2, (National Academy Press, 2002), *available at* http://bob.nap.edu/html/youth_Internet/.
 22. *Id.*
 23. *See id.*
 24. Lawrence Lessig, *Constitutional Law and the Law of Cyberspace*, in NATIONAL RESEARCH COUNCIL (U.S.), COMMITTEE TO STUDY TOOLS AND STRATEGIES FOR PROTECTING KIDS FROM PORNOGRAPHY AND THEIR APPLICABILITY TO OTHER INAPPROPRIATE INTERNET CONTENT STAFF(CB), TECHNICAL, BUSINESS, AND LEGAL DIMENSIONS OF PROTECTING CHILDREN FROM PORNOGRAPHY ON THE INTERNET : PROCEEDINGS OF A WORKSHOP 110, 111 (Washington, DC, USA; 2002); *available at* http://newton.nap.edu/html/protecting_children/ch17.html.
 25. *Ashcroft III*, 542 U.S. 656, 685 (2004).
 26. Merlis, *supra* note 10, at 128.
 27. *See* THORNBURG, *supra* note 20.
 28. *Id.*
 29. *Id.*
 30. *Ashcroft III*, 542 U.S. at 685.
 31. THORNBURG, *supra* note 20.
 32. *See id.*
 33. *Id.*
 34. Merlis, *supra* note 10, at 129.
 35. Robert Peters, *Once Again, U.S. Supreme Court Thinks It Knows Better than Congress*, 10 NEXUS 5, 6 (2005), *available at* <http://www.nexusjournal.org/2005obscurity/5-19.pdf>.
 36. Daniel Okrent, *Raising Kids Online*, TIME MAGAZINE, May 10, 1999, *available at* <http://www.time.com/time/archive/preview/0,10987,990919,00.html>.
 37. *See* Adele Horin, *Kids Drawn into Vile Web Porn as 60's Generation Sits on Its Hands*, SYDNEY MORNING HERALD., Mar. 3, 2003, at 1, *available at* <http://www.smh.com.au/articles/2003/03/02/1046540073744.html>.
 38. *Id.*
- Press Release, Nielsen/NetRatings, Three out of Four Americans Have Access to the Internet, According to Nielsen/NetRatings (March 18, 2004) (on file with author), *available at* http://www.netratings.com/news.jsp?section=new_pr.
39. [news.jsp?section=new_pr](http://www.netratings.com/news.jsp?section=new_pr).