UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Docket No. 020514121-2121-01

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER AND THE AMERICAN CIVIL LIBERTIES UNION ON THE EFFECTIVENESS OF "INTERNET PROTECTION MEASURES"

In response to NTIA's "Request for Comment on the Effectiveness of Internet Protection Measures and Safety Policies," 67 Fed. Reg. 37396 (May 29, 2002), the Electronic Privacy Information Center ("EPIC") and the American Civil Liberties Union ("ACLU") submit these comments to address the demonstrated, inherent flaws in content blocking systems and other so-called "Internet protection measures."

In furtherance of its proceeding "to evaluate whether currently available Internet blocking or filtering technology protection measures and Internet safety policies adequately address the needs of educational institutions," as required by the Children's Internet Protection Act ("CIPA"), Pub. L. No. 106-554, 114 Stat. 2763, 2763A-336 (2000), NTIA seeks comments on, *inter alia*, the following questions:

> - How do technology protection products block or filter prohibited content?
>
> - Do these methods successfully block or filter prohibited online content? [1]

These questions recently received extensive consideration by a three-judge federal court panel during the litigation of the constitutional challenge to CIPA's requirement that libraries install blocking software in order to qualify for participation in the E-Rate program.[2] The court showed — and we agree — that blocking methods currently in use block access to a large amount of online content permissible under CIPA (i.e. they "overblock"), while failing to block access to a large amount of online content prohibited by CIPA (i.e., they "underblock"). Because current blocking methods overblock permissible speech

---

[1] Request for Comment, 67 Fed. Reg. at 37398.

[2] *American Library Association v. United States,* 201 F. Supp.2d 401 (E.D. Pa. 2002) (*notice of appeal filed June 20, 2002*).

and underblock prohibited speech, they fail to “successfully block or filter prohibited online content.” In the remainder of this comment, we will use the court’s decision to illustrate why this is so.

The court noted that, "following an intensive period of discovery . . . the court conducted an eight-day trial at which [the court] heard 20 witnesses, and received numerous depositions, stipulations and documents. The principal focus of the trial was on the capacity of currently available filtering software."[3] This examination resulted in extensive findings of fact on the nature of blocking software, its operation, and the limits of the technology. These inherent technological limitations, the court held, make it impossible for a public library to comply with CIPA without violating the First Amendment.[4] (A copy of the court's decision is being filed herewith for inclusion in NTIA's record.)

The court's findings of fact, as summarized below, were based primarily on depositions and testimony concerning the content blocking provided by four tools: SurfControl's Cyber Patrol, N2H2's Bess/i2100, Secure Computing's SmartFilter and Websense's Enterprise. The court's findings contain general information concerning the blocking methods used by these companies, and assess the broader implications of "the sources of error that are at once inherent in those methods and unavoidable given the current architecture of the Internet and the current state of the art in automated classification systems."[5]

I. How Technology "Protection" Products Work.

Conceptually, blocking programs function in a straightforward manner. "When an Internet user requests access to a certain Web site or page, either by entering a domain name or IP address into a Web browser, or by clicking on a link, the filtering software checks that domain name or IP address against a previously compiled 'control list.'"[6] If the control list

[3] *Id.* at 407-408.

[4] *Id.* at 453 ("Because of the inherent limitations in filtering technology, public libraries can never comply with CIPA without blocking access to a substantial amount of speech that is . . . constitutionally protected . . .").

[5] *Id.* at 430.

[6] *Id.* at 428.

responds that the address is restricted, then the user will not be allowed to access it.

As the blocking software companies review individual Web sites or pages, they place the address (URL) into content categories within the control list. For example, SurfControl uses 40 different content categories such as Adult/Sexually Explicit; Education; Real Estate; and Violence. The administrator of the blocking software then has the ability to restrict access to specific categories, and all of the web addresses included therein.[7]

Therefore, when gathering the URLs to place onto the control lists, blocking software companies go through two distinct phases. "First, they must collect or 'harvest' the relevant URLs from the vast number of sites that exist on the Web. Second, they must sort through the URLs they have collected to determine under which of the company's self-defined categories (if any), they should be classified."[8] [9] The methods used in both of these phases are, however, flawed and thus unsuccessful at controlling access to restricted materials while improperly blocking access to a vast amount of valuable content.

II. The Harvesting Phase is Flawed.

The harvesting phase introduces flaws into content blocking because it only considers a small proportion of relevant URLs. An effective control list should include the full universe of currently available web addresses. However, "filtering companies, given their limited resources, do not attempt to index or classify all of the billions of pages that exist on the Web. Instead, the set of pages that they attempt to examine and classify is restricted to a small portion of the Web."[10] SurfControl, N2H2 and Secure Computing maintain control lists with only 200,000 to 600,000 web addresses,[11] a miniscule number

---

[7] *Id.*

[8] *Id.* at 430.

[9] Automated methods used in the process of sorting or "categorizing" URLs are discussed further in Section III.B, *infra*.

[10] *Id*. at 431.

[11] *Id.* at 428.

given that the number of pages that can be accessed by standard search engines has been estimated at 2 billion pages.[12]

The control lists contain so few web addresses because the automated and manual search methods blocking software companies use to find Web pages are imperfect. The bulk of the web addresses are gathered through automated methods such as "entering certain key words into search engines [and] following links from a variety of online directories (e.g., generalized directories like Yahoo or various specialized directories, such as those that provide links to sexually explicit content)."[13] These are then supplemented by manually "reviewing lists of newly-registered domain names; buying or licensing lists of URLs from third parties; 'mining' access logs maintained by their customers; and reviewing other submissions from customers and the public."[14]

A. Keyword Searching at Commercial Search Engines Only Searches a Small Proportion of All Web Addresses.

As the court found, "the first method, entering certain keywords into commercial search engines, suffers from several limitations. [T]he Web pages that may be 'harvested' through this method are limited to those pages that search engines have already identified. However, . . . a substantial portion of the Web is not even theoretically indexable."[15]

In addition to the 2 billion web pages that blocking software companies could reach through keyword searching, there are at least a similar number of pages which cannot be reached through commercial search engines. The court found that "the size of the un-indexable Web, or the Deep Web, while impossible to determine precisely, is estimated to be two to ten times that of the publicly indexable Web."[16] Thus, keyword searching, based upon the estimates credited by the court, could at best reach a very small percent of all Web pages. As the court found, "no

---

[12] *Id.* at 419.

[13] *Id.* at 431.

[14] *Id.*

[15] *Id.*

[16] *Id.* at 419.

currently available method or combination of methods for collecting URLs can collect the addresses of all URLs on the Web."[17]

B. Keyword Searching at Commercial Search Engines Doesn't Identify Visual Depictions.

The second drawback of relying upon automated methods is that they use text as a proxy for finding visual content. The commercial search engines are only able to search text, not images. As the court noted, "[t]his is of critical importance, because CIPA, by its own terms, covers only 'visual depictions.'"[18] The court found that

> [i]mage recognition technology is immature, ineffective, and unlikely to improve substantially in the near future. . . . Due to the reliance on automated text analysis and the absence of image recognition technology, a Web page with sexually explicit images and no text cannot be harvested using a search engine. This problem is complicated by the fact that Web site publishers may use image files rather than text to represent words, i.e., they may use a file that computers understand to be a picture, like a photograph of a printed word, rather than regular text, making automated review of their textual content impossible. For example, if the Playboy Web site displays its name using a logo rather than regular text, a search engine would not see or recognize the Playboy name in that logo.[19]

For these reasons, control lists are both insufficient and inaccurate as a result of flaws in the harvesting process. By accessing less than 20 percent of Web addresses, and returning only those that use descriptive text, harvesting produces incomplete control lists. Such incomplete lists lead to the phenomenon of underblocking, where blocking programs fail to block Web sites containing content that should be blocked according to the program's stated criteria.

III. The Categorization Phase Introduces Flaws.

---

[17] *Id*. at 418.

[18] *Id.* at 431.

[19] *Id.* at 431-432.

Flaws in the process of categorizing harvested Web sites lead to the phenomenon of overblocking, where content that should not be blocked is miscategorized as content that should be blocked. An expert witness for the government admitted that six to fifteen percent of the Web pages blocked on library computer terminals are wrongly blocked. The court found, however, that these already substantial estimates "greatly understate the actual rates of overblocking that occurs, and therefore cannot be considered as anything more than minimum estimates of the rates of overblocking that happens in all filtering programs."[20] Therefore, *at least* fifteen percent of the Web pages blocked in libraries using blocking software are wrongly blocked. The court further found that the thousands of overblocked Web pages identified by plaintiffs' experts were only a small fraction of those that are actually overblocked: "[W]e conclude that many times the number of pages that [plaintiffs] identified are erroneously blocked by one or more of the filtering programs that [were] tested."[21]

The court cited many specific examples of "overblocking," including Web pages containing information about religious organizations (e.g., the Web site of the Knights of Columbus Council 4828, a Catholic men's group associated with St. Patrick's Church in Fallon, Nevada), governmental entities and specific political candidates (e.g., the Web site for Kelley Ross, a Libertarian candidate for the California State Assembly), health issues (e.g., the Web site of the Willis-Knighton Cancer Center, a cancer treatment facility), education and careers (e.g., several Web sites with information on home schooling, and a site for aspiring dentists), travel and sports (e.g., the Web sites of a North Carolina bed & breakfast and a fly-fishing outfitter in Alberta).[22] The cause of such overblocking can be traced to the following flaws in the categorization process used by blocking software companies.

A. The Category Definitions are Inaccurate.

The categories for content that blocking companies use are inconsistent with those categories identified in CIPA, and as a result, they block content permissible under CIPA. After

[20] *Id.* at 442.

[21] *Id.* at 445.

[22] *Id.* at 446-447.

blocking software companies use the above-described methods to compile control lists, they allocate the URLs to different content categories. For example, Websense uses the following headings: Abortion Advocacy; Advocacy Groups; Adult Material; Business & Economy; Drugs; Education; Entertainment; Gambling; Games; Government; Health; Illegal/Questionable; Information Technology; Internet Communication; Job Search; Militancy/ Extremist; News & Media; Productivity Management; Bandwidth Management; Racism/Hate; Religion; Shopping; Society & Lifestyle; Special Events; Sports; Tasteless; Travel; Vehicles; Violence; and Weapons.[23]

The blocking software companies do not define their categories according to legislative or common law definitions of prohibited materials. Obviously, none of Websense's above categories matches the prohibited categories of obscenity, child pornography and materials harmful to minors referenced in CIPA. The "Adult" category is defined as including "full or partial nudity of individuals." However, it also includes unprohibited content such as Web pages that contain "light adult humor and literature" and "sexually explicit language."

In addition, blocking software users are not generally allowed to either define categories for themselves or have access to the control lists and their categorizations. As the court noted, "the specific methods that filtering software companies use to . . . categorize control lists are, like the lists themselves, proprietary information."[24] Therefore, blocking software is, at the most, effective at blocking the categories as defined by the blocking companies, not the desired categories of a particular user, or those mandated by law.

By using category definitions, which cannot be meaningfully customized, that are much broader than the categories of content prohibited by CIPA, blocking software will necessarily overblock a large amount of content permissible under CIPA — even when the blocking companies' definitions are accurately applied. Of course, those definitions are not always accurately applied, as discussed below; content matching a category definition is often not placed in the appropriate category, while content not matching a category definition will often be categorized as such by mistake. These inaccurate categorizations lead to further overblocking and underblocking.

---

[23] *Id.* at 429.

[24] *Id.* at 430.

B. Automated Allocations Inaccurately Categorize URLs.

Both of the methods that blocking software companies currently use to automatically put a URL into one or more content categories result in overblocking of content permissible under CIPA, as well as underblocking of content prohibited under CIPA. Blocking software companies currently use two textual methods to automatically categorize addresses: simple key word searching, and statistical algorithms. The court found that "simple key-word-based filters are subject to the obvious limitation that no string of words can identify all sites that contain sexually explicit content, and most strings of words are likely to appear in Web sites that are not properly classified as containing sexually explicit content."[25] The court similarly found that the use of statistical algorithms yields flawed results:

> Notwithstanding their "artificial intelligence" description, automated text classification systems are unable to grasp many distinctions between types of content that would be obvious to a human. And of critical importance, no presently conceivable technology can make the judgments necessary to determine whether a visual depiction fits the legal definitions of obscenity, child pornography, or harmful to minors.[26]

C. Human Allocations are Unable to Efficiently and Accurately Categorize URLs.

Use of human review — as opposed to automated blocking — also results in the overblocking of content permissible under CIPA, as well as underblocking of content prohibited under CIPA. Most blocking software companies engage in some percentage of human review, in addition to their reliance upon automated methods. As the court noted, "[h]uman review of Web pages has the advantage of allowing more nuanced, if not more accurate, interpretations than automated classification systems are capable of making."[27] However, human review is unable to categorize many Web pages without incurring a significant rate of error.

---

[25] *Id.* at 432.

[26] *Id.* at 433.

[27] *Id.*

The enormity of the task of human review of billions of Web pages introduces its own sources of error. With limited resources, any attempt at human review of billions of existing web pages, and the approximately 1.5 million new Web pages created every day will introduce human error. The court found that "errors are likely to result from boredom or lack of attentiveness, overzealousness, or a desire to err on the side of caution by screening out material that might be offensive to some customers, even if it does not fit within any of the company's category definitions."[28]

The demands of human review also introduce two procedural errors. Often times, to cope with the demands of review, categorical determinations will be made not upon the basis of the content of each specific Web page, but based upon the site's home page.[29] Thus, if the home page of a Web site appears to be objectionable, all of the Web pages associated with that site will be categorized similarly. These broad determinations lead to over-blocking of many useful Web pages based upon a cursory review. In other cases, this practice allows justifiably prohibited content to remain unblocked. For example, a site which hosts the Web pages of thousands of individuals (or which charges for access) will not be reviewed thoroughly, and thus some of its content may be available for viewing notwithstanding the "inappropriate" nature of that particular material.

D. All Allocation Methods are Inaccurate Because They are Static While Web Content is Dynamic.

Blocking software companies do not have the resources or technological means to continually monitor Web page content, although that content changes daily. As the court found:

> Most filtering software companies do not engage in subsequent reviews of categorized sites or pages on a scheduled basis. Priority is placed on reviewing and categorizing new sites and pages, rather than on re-reviewing already categorized sites and pages. Typically, a filtering software vendor's previous categorization of a Web site is not re-reviewed for accuracy when new pages are added to the Web site. To the extent the Web site was previously categorized as a whole, the new pages added to the site usually share

[28] *Id.*

[29] *Id.* at 433-434.

> the categorization assigned by the blocking product vendor.[30]

The court further noted that, "in addition to the content on Web sites or pages changing rapidly, Web sites themselves may disappear and be replaced by sites with entirely different content. If an IP address associated with a particular Web site is blocked under a particular category and the Web site goes out of existence, then the IP address likely would be reassigned to a different Web site."[31] Likewise, "[t]hrough 'virtual hosting' services, hundreds of thousands of Web sites with distinct domain names may share a single numeric IP address." When blocking software companies block the IP addresses of such services, they "necessarily block a substantial amount of content without reviewing it, and will likely overblock a substantial amount of content."[32]

Thus, the categorization of URLs within control lists is inaccurate due to inherent flaws in the methods employed. Because the blocking software companies unilaterally determine the categories that can be blocked, and use inaccurate human and automated allocation methods, categorization produces highly unreliable results. When coupled with the insufficiency of the control lists, those results compound the inaccuracy of blocking systems.

IV. Less Restrictive, More Effective Means are Available.

Alternatives to Internet blocking software adequately address the needs of educational institutions seeking to comply with CIPA, as the court found. Many of the practices and policies considered by the court to be less restrictive in the library environment are either currently used or would be applicable to an educational environment. Schools can "adopt Internet use policies that make clear to patrons that the [school's] Internet terminals may not be used to access illegal content."[33] Other techniques recognized by the court, such as detecting violations of use policies through direct observation, review of Internet use logs, and subsequent disciplinary measures are all easily

---

[30] *Id.* at 435.

[31] *Id.*

[32] *Id.* at 434.

[33] *Id.* at 480.

adaptable to an educational environment. These methods would avoid the documented flaws of blocking software, while more effectively accomplishing the desired ends.

Conclusion

As the court concluded after an exhaustive examination of content blocking technology, "we find that it is currently impossible, given the Internet's size, rate of growth, rate of change, and architecture, and given the state of the art of automated classification systems, to develop a filter that neither underblocks nor overblocks a substantial amount of speech."[34] The court stressed that these problems are inherent to the blocking process, and not the result of deficiencies in particular programs:

> The more effective a filter is at blocking Web sites in a given category, the more the filter will *necessarily* overblock. Any filter that is reasonably effective in preventing users from accessing sexually explicit content on the Web will *necessarily* block substantial amounts of non-sexually explicit speech.[35]

NTIA should adopt the court's findings and conclude that currently available Internet blocking software does not "successfully block or filter" the online content that CIPA prohibits, and that use of such software is antithetical to the educational mission of the nation's schools.

Respectfully submitted,

David L. Sobel
Electronic Privacy Information Center

Laura W. Murphy, Director
ACLU Washington National Office

Greg Pemberton
EPIC Legal Intern

August 27, 2002

[34] *Id.* at 437.

[35] *Id.* (emphasis added).