Written testimony of Bennett Haselton, Webmaster and Co-ordinator, Peacefire.org

Commission on Child Online Protection

August 3, 2000

My name is Bennett Haselton and I have been operating the Peacefire.org Web site since it was created in August 1996. Peacefire was founded at a time when the Communications Decency Act of 1996, a law which prohibited the posting of "indecent" content on the Internet where it could be accessed by minors, had just been struck down by a three-judge panel in Philadelphia. At the time, most of the debate over Internet censorship censored on the rights and interests of adults. Peacefire.org was created to represent the interests and free speech rights of Internet users under the age of 18, a point of view that was almost completely unrepresented at the time.

As a result, our research focuses mostly on blocking software programs and other measures designed to restrict information from Internet users under 18. We focus almost exclusively on *overblocking*, the issue of non-pornographic sites that get blocked by blocking software, rather than *underblocking*, the issue of pornographic sites that do not get blocked. This focus reflects the belief held by most Peacefire members that pornography and profanity are not as "harmful" or "dangerous" as some politicians and blocking software companies have made them out to be, so we do not see underblocking as the most serious problem. On the other hand, I personally believe it can be very harmful to use blocking software to block sites and thereby *teach* a young user that the political, medical, and activist Web sites commonly blocked by blocking software, are "dangerous" or "immoral", without applying any critical thinking to that belief; hence our focus on overblocking.

So, this testimony will focus on the kind of sites that are usually "overblocked".

Sites that are usually "overblocked" by blocking software

When a blocking program blocks a site that does not fall into the categories of sites that a user would expect to be blocked (pornography, bomb-making, etc.), the site usually falls into one of these categories:

- sites blocked for political reasons
- sites blocked due to word or phrase blocking
- sites blocked due to sharing an IP address with another blocked site
- sites blocked with no apparent explanation

<u>Sites blocked for political reasons</u>

These sites can be further divided into two categories: political sites that are blocked as a matter of policy by the blocking software company, and political sites that are blocked but should *not* be blocked under the company's policy. If a political site is blocked as a matter of policy, then complaining to the company about the blocked site will usually not

get it unblocked. On the other hand, if a political site is blocked when it shouldn't be, the company will usually unblock it when the mistake is pointed out to them (after that happens, there is sometimes a problem that the company may not admit that the site was ever blocked at all, if the mistake is embarrassing enough that it might cause a political backlash). We consider these two categories separately – "Political sites blocked as a matter of policy", and "Political sites blocked in contradiction with the company's policy". For both of these categories, we only consider sites that are blocked for their political content, not political sites that are blocked due to keyword blocking (such the ACLU Web site being blocked by ClickSafe because of the word "gay/lesbian" on the main page).

Political sites blocked as a matter of policy

Of all the popular blocking software programs, the one with the worst reputation for political blocking is CYBERsitter; even organizations such as FilteringFacts.org that support blocking software, have distanced themselves from this company. CYBERsitter is the only major program whose policy officially supports the blocking of Web pages that support gay rights, including the National Organization for Women (NOW.org), the Gay and Lesbian Alliance Against Defamation (GLAAD.org), and the International Gay and Lesbian Human Rights Commission (IGLHRC.org). CYBERsitter even filters out the phrase "gay rights" from Web pages, so the sentence "Al Gore supports gay rights," would be rendered as "Al Gore supports."

Many blocking companies also include a category for drug-related Web sites, and sites such as the National Organization for the Reform of Marijuana Laws (Natlnorml.org) are often blocked under these categories. Such sites exist to advocate a political point of view in favor of marijuana legalization; as such, a public school or library that blocks these sites, while allowing students or patrons to view sites that oppose marijuana legalization, could potentially face a First Amendment lawsuit for viewpoint discrimination. (Some companies such as Cyber Patrol claim that their "drug sites" category does not block political sites that discuss drug laws. Third parties have nonetheless discovered political sites such as DrugLibrary.org to be blocked by Cyber Patrol in their "Drugs/Alcohol" category, but Cyber Patrol considers these blocks to be errors and usually corrects them, so these do not fall under "sites blocked as a matter of policy".)

It is much rarer for conservative sites to get blocked, but it did happen in one case as a result of an experiment that Peacefire conducted. In May, Peacefire published a report called "Project Bait And Switch", concluding that the six blocking software companies tested in our experiment – Cyber Patrol, SurfWatch, CYBERsitter, Net Nanny, WebSENSE and SmartFilter – demonstrated a double standard in deciding what sites to block.

Originally we had visited the Web sites of the Family Research Council (FRC.org), Dr. Laura Schlessinger (DrLaura.com), Focus on the Family (Family.org) and Concerned Women for America (CWFA.org) and found some of the anti-gay quotes that appeared

on the pages, such as "We believe that homosexuality is immoral, unhealthy, and destructive to individuals, families and socities," from the Family Research Council. We copied these quotes to separate Web sites on free-page servers such as GeoCities, without attributing them to their original source. When we submitted these URL's on the free-page sites to the six blocking software companies, all six companies replied and said that they would block the nominated URL's as "hate speech" because of their derogatory anti-gay statements. But when we revealed that we had copied the statements from other Web pages, all six companies declined to block the conservative sites that were the original source of the quotations.

We think the best testimony to the power of "Project Bait And Switch" is the fact that, of all the reporters which have contacted the different blocking companies to ask for their response to our report, none of the reporters have ever received a response (except from Net Nanny, which has said that blocking the original "bait" sites with the quotes on them, was probably a mistake). In the absence of any explanation from the blocking software companies, we believe that they decided not to block Dr. Laura, the Family Research Council, etc. because of the potential public relations backlash and the possibility of a boycott. The experiment shows what we believe to be a double standard for blocking political Web sites, based on the clout of the organization.

Political sites blocked in contradiction with the company's policy

As noted earlier, CYBERsitter blocks gay rights pages as a matter of policy, but most other products have also blocked pages related to gay rights issues as well. The difference is that most other companies – Cyber Patrol, N2H2, and SurfWatch, for example – will usually un-block these sites after being made aware of the error. The question remains: How did those sites get blocked in the first place?

Most blocking companies use a staff of reviewers who can add sites to the master database of blocked sites used by the company, so it is possible for an employee to misinterpret the company's blocking criteria and add a gay rights page to the company's "sexually explicit" list. Besides being blocked by CYBERsitter, the National Organization for Women page has been blocked in whole or in part by I-Gear, Net Nanny, and NetRated (but these companies, unlike CYBERsitter, removed the block once it was made public). Other gay rights pages blocked by other programs have included "Community United Against Violence" (a group against anti-gay violence), "Dutch Organization for Integration of Homosexuality (COC)" (a gay rights group in the Netherlands), "Lambda" (a Canadian gay rights group), Youth.org (a political advocacy and support site for gay teenagers), "Illinois Federation for Human Rights", and others listed on Peacefire.org and Censorware.org.

Again, except for the sites blocked by CYBERsitter, these were all considered by the blocking companies, and were later unblocked. But given the small samples that Peacefire looked at to find these blocked sites – compared against the size of the huge databases used by most blocking companies – there is no way to know how many more sites are incorrectly blocked and simply haven't been discovered yet. An over-eager site

reviewer, working for a blocking software company, could sincerely believe that they are doing their job accurately when they add a gay rights page to the company's "sexually explicit" database.

On the other hand, there are also sites that get blocked which no company employee could believe are appropriate for blocking; the employee may simply add the site to the company's database out of spite. This seems likely in the case of, for example, X-Stop blocking the affirmative action department of Winona State University in Minnesota. We confirmed that the URL itself was blocked by the program, and the page was not getting blocked due to any bizarre "keyword filtering". Since X-Stop does not have a policy of blocking affirmative action sites, the URL was apparently added to their database by a "renegade" employee who opposed affirmative action.

The reports on Censorware.org and Peacefire.org give many more examples of sites that are blocked due to political content.

Sites blocked due to word or phrase blocking

These are the examples which are most popular with the media. This year, columnists and radio commentators made much of the fact that Beaver College in Pennsylvania was changing its name after years of snickering and dirty jokes, also noting that many high school students were being blocked from doing Web searches on the phrase "Beaver College". Many library patrons reported being blocked from sites about "Super Bowl XXXIV" because of the "XXX" in the title. Librarians have pointed out since the beginning of the debate over blocking software that "breast cancer" sites and "chicken breast recipes" are often blocked. In reports that we sent to the COPA Commission in July, we found that the home page of Lawrence Lessig, one of the testifying witnesses, was blocked by ClickSafe.com (another company represented at the same hearing) because of the word "cocktail" on Professor Lessig's page.

Although Peacefire does publish examples of such sites being blocked, I think it is unfortunate that these "keyword blocks" receive such a disproportionate amount of attention, because they do not illustrate the real problems with blocking software. When a site like "Super Bowl XXXIV" is blocked, it is obviously blocked due to a shortcoming in the blocking program, and *not* due to any political bias on the part of the manufacturer. The fact that a program blocks the ACLU home page for its political content, is much more damning than the fact that they block "Super Bowl XXXIV" by accident. And yet even librarians who oppose the use of blocking software will often say that they reject it because it "blocks chicken breast recipes" or "blocks sites about breast cancer". Since these librarians would presumably be justifying their position more strongly if they pointed out the fact that sites like NOW.org and ACLU.org are blocked, I believe that the reason more librarians (and other blocking software opponents) fail to point this out, is because they don't know about it. This is why I think that keyword blocks like "Beaver College" are receiving too much attention, while the more politically motivated blocks are not getting enough discussion.

On the other hand, there is one type of keyword blocking that I think *should* receive more attention than it does, and which reflects poorly on the companies that have been caught implementing it. This involves companies that use special computers or "spiders", located on their own networks, to explore the Web and search for pages containing certain keywords. If a site containing these keywords is found, it is added to the company's list of pornographic Web pages, and the list is propagated to users of the blocking program. Humans are conspicuously absent from this process; the site is *not* reviewed by a human being first before it is added to the list.

This is a serious problem because:

- If the company has stated that they always review sites before adding them to their list, then that statement from the company is false, if they are adding sites to their list without reviewing them first.
- If the product guidelines say that "Keyword blocking is optional and can be turned off", this is misleading because if a site has been added to the company's *list* of "bad sites" due to keywords, it will still be blocked even if "keyword blocking" is turned off.

For example, Cyber Patrol once blocked a Web site called MapleSoccer.org, a youth soccer league in Massachusetts, which does not contain any content that could be considered even remotely offensive. When the Censorware Project discovered that this site was blocked, it took some time to figure out why: the page included links to the different teams in the league, and links were captioned "Boys under 12", "Boys under 10", etc. – causing the Cyber Patrol spider to flag the page as a "child pornography" site. Thus, the site had been added to Cyber Patrol's "sexually explicit" list, even though it was clear that no human being could have reviewed the page first.

Another example was a site called "WebDevil.com", blocked by Cyber Patrol in their "Satanic/Cult" category; WebDevil is actually a Web design firm. Again, no human being could have reviewed the site and added it to the "Satanic/Cult" category, but the word "devil" in the page title apparently caused it to be added to Cyber Patrol's list.

Peacefire.org and Censorware.org contain more examples of sites blocked due to keyword blocking.

<u>Sites blocked due to sharing an IP address with another blocked site</u>

Many blocking software programs, notably SurfWatch, block sites by IP address instead of by host name. (The IP address for a site is a set of four numbers like "206.251.29.10" that is used by actual Internet software; the "hostname" is the human-readable name like www.playboy.com.) Many Internet service providers host multiple sites on the same IP address, and if SurfWatch blocks one site on that address, all the other sites on that address will be blocked as well.

The most ironic example of a site blocked for this reason was probably FilteringFacts.org, a pro-blocking-software site that actually lists SurfWatch under

"recommended filters". FilteringFacts.org was blocked under SurfWatch's "Drugs/Alcohol" category, because of another site on the same server that had been classified under that category.

Peacefire also found recently that the Electronic Frontiers Australia site (www.efa.org.au), Australia's foremost organization opposing Internet censorship, had been blocked by SurfWatch after the EFA relocated their Web site to a hosting company in the United States. (Ironically, the EFA moved their site to the U.S. to evade Internet censorship laws that had just been passed in Australia.) Since SurfWatch did not block the EFA site before it was relocated, it seemed apparent that the site was now blocked because it was located on a new IP address, which was shared with other existing Web sites.

Sites blocked with no apparent explanation

These are sites consisting of content that could not possibly considered offensive to anyone, even from an extremist political point of view, and have still been found to be blocked by the different blocking programs. This is a catch-all for blocked sites listed on Peacefire.org and Censorware.org that cannot be explained in any other category. Jonathan Wallace published an essay in 1997, "The X-Stop Files", describing sites he had discovered to be blocked by X-Stop including the Quakers home page. We also found X-Stop to be blocking the Bling Children's Center of Los Angeles (http://www.blindcntr.org/bcc/) and the San Jose Mercury News online (http://www.sjmercury.com/) – neither being the kind of site that anyone could consider offensive or even politically disagreeable.

Censorware.org and Peacefire.org have many more examples of sites blocked in all five of these different categories. Also, you can usually find a few examples of your own by downloading and installing a blocking program, and leaving it running for some time while you attempt to continue with your normal Web surfing and research.

Conclusion

It is a cliché to point out that, given the size of the Web (over one billion pages by almost all estimates) and its rapidly changing nature, no company can accurately classify it all. Blocking software companies should not be held responsible for the fact that their products do not – indeed, cannot – work accurately for the entire Web.

But companies *should* be held responsible for statements that they make about their products which are not supported by evidence. For SurfWatch and Cyber Patrol, for example, their claims that "every page on our list is reviewed by a human first" have been contradicted by several published reports of sites blocked by their software. X-Stop once made the same claim, but they retracted it after numerous examples of wrongly blocked sites were introduced as evidence in *Mainstream Loudoun v. Board of Trustees*, a successful First Amendment lawsuit filed against the Loudoun County, VA library system after they installed X-Stop on their terminals. The testimony that Richard

Schwartz, CEO of ClickSafe.com, gave before this commission, stating that ClickSafe achieves “extraordinarly high rates of accuracy” in filtering content, is called into question by the fact that about 50% of the pages on COPACommission.org were blocked by his software.

Blocking software companies should also be held responsible for flaws in their product that should have been discovered during a testing phase before the software was released. Normally, if I buy a program that costs $30 or $40 (about the cost of most blocking software packages), it might take a few hours or a few days to find a serious defect in the software, and over the course of a few months, I might only find about a dozen serious problems that I think the manufacturer should have discovered.

On the other hand, after I install a new blocking software program, it is easy to find thirty or forty wrongly blocked sites in a few hours. Most of these mistakes are acknowledged as mistakes by the manufacturer and later corrected – but the company could have found most of the mistakes on their own, if they had asked a user to test the program for a few hours looking for wrongly blocked sites, before the program was released. (In fact, the blocking company ought to be able to find the mistakes even faster, since they have access to the list of blocked sites, while outside customers cannot see the list and have to find blocked sites by trial and error.) Since this kind of testing work does not require an experienced programmer, it could have been done by an intern working at $10 per hour, for a total cost of about $100. So it is sadly ironic that many of the mistakes which Peacefire has found and publicized in different blocking programs, could have been found and corrected if the company had been willing to spend $100 to test the program for “overblocking” before releasing it. We regret to conclude that blocking software companies in general are not very concerned about overblocking in their products.