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

RESPONSE TO WRITTEN QUESTIONS OF JUNE 5, 2003

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

June 30, 2003

The Question Posed by the Copyright Office

On June 5th, 2003, the Copyright Office asked the opponents of the proposed exemption for "Compilations consisting of lists of websites blocked by filtering software applications" for our response to the following:

> *Please clarify, as specifically as possible, the types of applications you believe should or should not be subject to an exception for the circumvention of access controls on filtering software lists, if such an exception is recommended.*
>
> *Please provide any documentation and/or citations that will support any of the factual assertions you make in answering these questions.*

The opponents of the exemption do not believe any exemption is justified because there is no supporting record to justify it. The opponents further believe that a narrowed exemption designed to exclude "security suite" applications that include lists of blocked websites would unfairly render the databases of some vendors of lists of blocked websites with protection and others without on an arbitrary basis.

A "security suite" exemption would result in the intervention by the Copyright Office in the ongoing evolution of the security software industry controversy of "best of breed" vs. "security suite." Ironically, such a "security suite" exemption would actually be counter to the interests of the proponents, as it would leave the three largest vendors of filtering software without a DMCA exemption.

The opponents further argue that the record developed during the 2003 hearings by the Copyright Office documents both the widespread and easy accessibility of tools for analyzing and criticizing filtering software, as well as the potential harm for allowing an exemption.

For these reasons, the proposed exemption should be denied.

Problems with Narrowing the Exemption to Exclude "Security Suites"

Arguing on behalf of a coalition of copyright owners, Steve Metalitz stated in his May 14, 2003 testimony before the Copyright Office:

> *We know that filtering software that may fit the description that appears in the exemption that exists now is one of the key tools in keeping our network safe and secure. And many of those filtering software packages may include lists of websites that either are the sources of viruses or the source of SPAM, which is of course is a scourge that we're all having to deal with increasingly now. In other words, that programs that really I don't think anyone in Mr. Tyre's would consider censorware may be swept within the ambit of this exception with potentially very serious consequences in terms of compromising the security and safety of computer networks.*[1]

It is our view that Mr. Metaliz is correct in this assertion. In order to deal with emerging security threats, major secure content management vendors must include "Compilations consisting of lists of websites blocked by filtering software applications." The analyst bulletin prepared by IDC, "Worldwide Secure Content Management Software Market Forecast and Analysis, 2002–2006: Vendor Views," provides some useful background.

IDC summarizes the evolving technology of anti-virus vendors:

> *Blended threats such as Nimda, Goner, and Code Red have become increasingly more common. A blended threat is a complex virus or worm program that targets multiple weaknesses in computer networks and is capable of doing damage in multiple ways.*
>
> *Unlike traditional viruses, which rely on the user to spread the infected files, blended threats are automated and are always scanning the Internet and local networks for vulnerabilities and other computers to infect; that is, they spread without user interaction.*
>
> *Since blended threats are designed to get past point-solution security systems, there will be a strong push toward a "layered security" approach that will be better able to combat blended threats. The layered security approach will combine solutions such as desktop antivirus, server and gateway antivirus (e.g., email), content filtering, vulnerability management, intrusion detection, and firewalls.* [2]

This "layered approach" often takes the form of the "security suite." A security suite is a single, integrated product that offers multiple security functions such as anti-virus filtering, spam filtering, intrusion detection -- and web content filtering.

Web content filtering is part of a broader software category referred to as "secure content management," as defined by IDC:

> *Secure content management is an emerging market that reflects corporate customers' need for a policy-based Internet management tool that addresses virus protection, Web content, email scanning, and downloadable applications*

> *execution. Secure content management technologies cover three specific product areas: antivirus software (AV), Internet access control and employee Internet management (IAC/EIM), and email scanning.*[3]

IDC documents the market position of the secure content management field. Four companies dominate the overall market share in secure content management: Symantec, Network Associates, Trend Micro, and Computer Associates.[4] These four companies all offer web content filtering as part of integrated security suites.

Symantec

Symantec sells an integrated suite product that includes web content filtering called "Symantec Gateway Security," which is described on the Symantec website:

> *Delivers comprehensive gateway protection in an easy-to-manage appliance designed to meet the unique security needs of small and medium-sized offices as well as branch locations. Provides protection against the latest Internet-based threats with fully integrated firewall, antivirus, Internet content filtering, intrusion detection, and virtual private networking technologies.*[5]

Trend Micro

Trend Micro sells an integrated suite product that includes web content filtering called "InterScan™ WebManager™," which is described on the Trend Micro website. Note that Trend Micro integrates the filtering list of Cyber Patrol:

> *InterScan™ WebManager™ blocks unproductive URLs, monitors and manages Web usage, and scans Web traffic for viruses and other malicious code at the gateway. InterScan WebManager combines comprehensive, antivirus technology, Web monitoring, and management tools from Trend Micro™ with extensive URL filtering and URL libraries from Cyber Patrol™ to help ensure that Internet resources are used safely and productively.*[6]

Network Associates

Network Associates sells an integrated suite product that includes web content filtering called "McAfee ® WebShield ®," which is described on the Network Associates website:

> *The McAfee ® WebShield ® appliances are integrated solutions, combining award-winning anti-virus and content management software with enhanced hardware. Tuned for performance, the WebShield e250, e500, and e1000 appliances offer McAfee anti-virus protection to quickly resolve your major business virus security worries.*[7]

Computer Associates

Computer Associates sells an integrated suite product that includes web content filtering called " *e*Trust Intrusion Detection," which is described on the Computer Associates website:

> e*Trust Intrusion Detection is a complete session security solution that incorporates three key security capabilities into one package — comprehensive network protection, network session monitoring and Internet content blocking.*[8]

Further complicating the issue of separating "pure filtering companies" from "security suites" is the fact that a number of these security suite products integrate filtering lists from "pure filtering companies." As is noted above, the filtering company Surfcontrol resells its Cyber Patrol list to Trend Micro for inclusion in its suite.

N2H2 also follows this practice by reselling its filtering list to NetIQ for inclusion in the NetIQ WebMarshall security product, as described on the NetIQ website:

> *NetIQ WebMarshal is an employee Internet management solution designed to promote responsible Web use while providing protection from viruses, confidentiality breaches and downloading of non-business material. The N2H2 Filtering List delivers enhanced web filtering capability with automatic daily updates and set & forget administration..*[9]

The situation is complicated even further by the fact that some traditionally "pure" filtering companies are now offering suite products. The filtering company Websense recently released a security suite product in a June 5, 2003 press release:

> *Websense Enterprise Security Suite™ Stops Spread of Web-Based Viruses and Malware; Complements Anti-Virus Software With Desktop Protection*
> *New Class of Malware Highlights Need for Additional Layers of Security*
>
> *SAN DIEGO, June 5, 2003 -- Websense Inc. (NASDAQ: WBSN), the world's leading provider of employee Internet management (EIM) solutions, today announces the availability of Websense Enterprise Security Suite.*
>
> *Designed to complement a company's existing anti-virus tools and protect a company's network from Web-based virus and malware infection before an updated virus signature becomes available, Websense Enterprise Security Suite combines the database categories of Websense Premium Group III – protection against Web-based viruses, malicious Web content and spyware – and the company's new Client Application Manager™ (CAM), an add-on module of Websense Enterprise v5 software.*[10]

Surfcontrol has also recently began offering a "Total Filtering Solution," as described on the company website:

> *SurfControl helps your company stop unwanted content. We offer Web, e-mail, and Instant Message filtering, the most comprehensive list of suspect URLs, and we employ intelligent, policy-driven technology that lets you manage the content on your network - even if you don't know exactly what that content will look like ahead of time.*[11]

According to market share data, the result of an exemption based on web content filtering offered as part of a larger integrated security product would mean that three of the top six filtering companies would be exempt and three would not. IDC ranks the market positions of the leading manufactures of web content filtering in the following order: SurfControl, Websense, Symantec, Secure Computing, N2H2, 8e6 Technologies.[12]

An exemption conveyed on some filtering companies but not others would unfairly punish "pure play" filtering companies by exposing their products to hacking and intrusion, while protecting "suite" products.

Further, this would insert the Copyright Office into an ongoing debate in the IT industry as to whether or not to use integrated suite software products or "best of breed" products. See, for example "Integrated Suites Vs. Best of Breed," ComputerWorld, February18, 2002, available at http://www.computerworld.com/softwaretopics/crm/story/0,10801,68240,00.html

A "security suite" exemption would also mean that some versions of filtering company databases would be exempt and some would not. As described above, N2H2 resells its database to NetIQ and SurfControl resells its database to TrendMicro.

Further, some of the opponents may in the future become producers of suite products. For example, Bsafe contains the following statement on its website regarding the future direction of the company:

> *The Future*
> *In addition to home filtering, reporting and protected email, in the future, Bsafe expects to regularly release new safety and security related services over the next several years. Bsafe will continue to improve its integrated firewall system, and is now distributing under license the sophisticated Nod32 virus control package for the Windows platform. Further Bsafe product releases will include services for child monitoring / predator detection and capture.* [13]

The above statement by Bsafe identifies yet another problem with the class of works opponents propose. Bsafe is sold to the home consumer market, and has not announced any plans to enter the public sector market of libraries, schools, and government.

But since the proponents have stated they are only concerned with filtering software that is sold in the public sector[14], why should companies like Bsafe be subjected to the exemption at all?

Proponents of the exemption have to date not provided any clarification for the Copyright Office to navigate through the complex topic of what constitutes a "compilation consisting of lists of websites blocked by filtering software applications." Therefore, proponents of the exemption have failed to meet their burden of defining a class of works.

First Amendment Concerns Expressed by Proponents are Misplaced

Proponents universally express the opinion that they are most concerned with the First Amendment issues related to the use of filters in the public sector. Notably, the recent decision by U.S. Supreme Court in the case ALA v. U.S. makes clear that First Amendment concerns are not applicable to the use of filtering software in public libraries. The view that the use of Internet filtering software does not violate the First Amendment rights of library patrons was held by the 6-3 majority who voted to uphold CIPA, and by one of the dissenters as well.

The majority opinion expressed by Chief Justice Rehnquist, joined by Justice O'Connor, Justice Scalia, and Justice Thomas, concluded:

> *Because public libraries' use of Internet filtering software does not violate their patrons' First Amendment rights, CIPA does not induce libraries to violate the Constitution, and is a valid exercise of Congress' spending power.*[15]

In a separate opinions, Justice Kennedy concurred the use of filters in libraries required by the act was constitutional:

> *…the statute is not unconstitutional on its face. For these reasons, I concur in the judgment of the Court.*

In a separate opinion, Justice Breyer concurred the use of filters in libraries required by the act was constitutional:

> *I therefore agree with the plurality that the statute does not violate the First Amendment, and I concur in the judgment.*

Additionally, Justice Stevens in dissent also expressed the view that the use of filtering software in libraries was constitutional:

> *I agree with the plurality that it is neither inappropriate nor unconstitutional for a local library to experiment with filtering software as a means of curtailing children's access to Internet Web sites displaying sexually explicit images.*

The proponents themselves have admitted that there is no justification for an exemption where the First Amendment is not applicable. From May 14, 2003 testimony of James Tyre:

> *We have never taken the position, I don't know anyone that's ever taken the position, that if a family chooses to use censorware in the home or if a private corporation chooses to use it at the workplace, that there are any First Amendment issues there. We may criticize it because we don't like censorware does, but we make no claims that there's any particular legal significance to it.*[16]

Since the U.S. Supreme Court has ruled definitively that First Amendment analysis is not appropriate to the use of filtering software, the Copyright Office need not give First Amendment concerns any consideration in determining the appropriateness of an exemption.

Concerns that CIPA Requires Schools and Libraries to Use "Closed Lists" are Misplaced

At the April 11th hearing, both proponents expressed the view that if the Children's Internet Protection Act (CIPA) were upheld, this would increase the justification for the exemption:

> *Mr. Band:...I also think that if the Supreme Court reverses the lower court in the CIPA decision, and then you start and then schools and libraries are required by law to use the filters, if they receive federal funding, I suspect at that point the public interest in the issue will rise significantly, and at that point the group of six might become twelve.*
> *Mr. Finkelstein: It might become a growth industry.*[17]

Although the Supreme Court has upheld CIPA, this in no way justifies the need to violate contract agreements and break into filtering software programs.

Schools and libraries that feel they must comply with CIPA in order to retain needed funds, but do not want to purchase a "closed list" filtering product can purchase "open list" or "open source" products and still be in compliance with CIPA. Opponents have identified three such "open list" products that are readily available to schools and libraries.

Two days after the CIPA decision, BioNet, the company which recently purchased the assets of the bankrupt Net Nanny, announced a marketing effort toward public libraries centered on the products "open list", that was reported widely by the *Associated Press*:

> *BioNet's Net Nanny program allows authorized users like parents or librarians to download lists of permitted and restricted Web sites and words, then add or subtract from that list. Tull said the feature should give the product an advantage in the minds of librarians and other critics who have likened filters to "electronic book burning."… NetNanny, which caters mainly to parents seeking safeguards for home computers, will make a major play for libraries, Tull said.*[18]

BioNet now features a promotional offer titled, "Net Nanny 5 is Your CIPA Compliance Solution," displayed on the BioNet website:

> *Net Nanny software meets the needs of libraries as it can be immediately and easily deactivated by an authorized individual at the request of adult library users, has the only fully viewable and editable lists of blocked websites, and readily makes available what criteria are used for filtering in its product documentation.*[19]

In addition to the commercial product offered by BioNet, two free products are also available. A recent issue of *Linux Journal* discusses these two solutions:

> *Maybe we need open-source censorware, strange as that may sound, with a publicly available list. It would offer the ability to tinker with both the code and the list to suit the needs of folks who have to do this type of work. I was stunned by the answer I found: two such animals already are available. One is Dan's Guardian, which I mentioned above; the other is squidGuard, a plug-in for the Squid web proxy.* [20]

SquidGuard is described on the website SquidGuard.org, which states that "the porn section of the blacklist has now more than 100,000 entries."[21] Dan's Guardian sells the "DansGuardian/squidGuard Managed URL Blacklist," which is "open source."[22]

Some schools and libraries are already using these products to comply with CIPA. The journal School Forge describes how the Meadville Public Library is using both Dan's Guardian and SquidGuard to comply with CIPA:

> *Because of the recent regulations in the U.S. resulting from the passage of the Children's Internet Protection Act, schools and libraries seem to be in the same circumstances in regards to filtering... since commercial filters are proprietary, in many cases the system administrator does not have the opportunity to modify or even view the lists of blocked sites, a.k.a. blacklists.*
>
> *At the Meadville Public Library, we are using two open source filters: squidGuard (www.squidguard.org) and DansGuardian (www.dansguardian.org). Both are available freely for download at the above Web sites, and they for the most part run on any open source operating system. Both are also server-based, making modifying the filtering organization-wide quick and simple.* [23]

The downside of these "open list" filtering products is that they are much less effective than commercial-grade filters with copyright-protected databases. The open list filter with the largest database is SquidGuard with 100,000 sites, much smaller than those of the main commercial filters, which have lists in the millions.

While these products are less effective than "closed list" products, the FCC has issued rules related to CIPA compliance that do not require any specific degree of effectiveness to comply with CIPA:

> *Some commenters have requested that we require entities to certify to the effectiveness of their Internet safety policy and technology protection measures. However, such a certification of effectiveness is not required by the statute. Moreover, adding an effectiveness standard does not comport with our goal of minimizing the burden we place on schools and libraries. Therefore, we will not adopt an effectiveness certification requirement.*[24]

It must be emphasized that there is no requirement to purchase "closed list" products anywhere in: 1) the language of CIPA; 2) the FCC's interpretation of CIPA, or 3) the Supreme Court's interpretation of CIPA.

Opponents Do Not Believe the Record Justifies an Exemption

The comments of the opponents make clear that the professional testing and research community views sampling as an adequate means for reaching conclusions about the public policy implications and controversies surrounding filtering software.

Nothing in the written or oral statements of Mr. Finkelstein, Mr. Tyre, or Mr. Band, or any of the parties favoring the exemption, takes serious issue with this observation. Rather, Mr. Finkelstein believes he is entitled to violate the copyright protection measures protecting filtering software because it is necessary for him to conduct deeper "architectural investigations" of filtering software. [25]

Mr. Finkelstein acknowledges that "architectural investigations" are not of interest to the research community, and are conducted by "maybe six people or so." [26]

While Mr. Finkelstein does not name these "six people or so," Mr. Tyre names five of them:

> *The Censorware Project is a group currently consisting of four people, myself, Jonathan Wallace, Jamie McCarthy, Bennett Hazelton. Originally there were two others, including Seth Finkelstein from whom you heard a great deal when you had a session in Washington.* [27]

The sixth individual who Mr. Tyre does not name is Michael Sims, who split from the Censorware.net and runs a rival site named Censorware.org. The site http://censorware.org maintained by Mr. Sims discusses the differences in philosophy and approach to studying filtering software and other issues that brought about the division in the Censorware Project.

These six individuals share a number of common characteristics. First, all six individuals have publicly expressed a strong philosophical opposition to filtering software. Second, all six individuals do not conduct research that is published in any peer-reviewed journal or other print publication, nor is their work cited by any peer-reviewed journal. Third, their research does not appear to employ any sort of scientific methodology, is apparently conducted on their personal computers, and is unaffiliated with any research or educational institution.

These points are documented by Michael Sims as he describes the formation of the Censorware Project on the http://Censorware.org website:

> *Let us start at the beginning. Way back when, some people all subscribed to an email list called "fight-censorship". The discussion part of the list is dead now; some part of it lives on as Politech. Before too long, some of the people on that list noticed that they all thought censorware was a bad thing. In a remarkable feat of self-organization, they decided to get together and try to raise public awareness. In alphabetical order: Seth Finkelstein, Bennett Haselton, Jamie McCarthy, Michael Sims, James S. Tyre, Jonathan Wallace.*
>
> *We worked by email - we lived in various places across the United States - and put together a report about the censoring software*[28]

After the split among the members of the Censorware Project in 2000, neither of two Censorware Project websites has conducted any research on filtering software during the exemption period, as Mr. Tyre admitted:

> *Mr. Tepp: Can you give us a sense of how many reports have been done in the last 3 years, or more precisely since October 29, 2000.*
> *MR. TYRE: Okay. Yes. Zero…our last report, which happened to be on Mr. Burt's company N2H2 was in 2000 but probably -- it was in 2000.*[29]

It is worth noting that the last Censorware Project report, "Passing Porn, Banning the Bible: N2H2's Bess in public schools," [30] was in fact published in 1999[31], and used a querying methodology, and did not rely on decryption.

Mr. Tyre does not provide any insight as to why educational institutions and research facilities do not feel that the research conducted by Censorware Project members is valuable, or why these institutions do not value decryption research. But Mr. Finkelstein does. Mr. Finkelstein stated in oral testimony that he believes that the research facilities that evaluate filtering software do not conduct his type of "architectural investigation" because they view this research as:

> *"something which might get me sued, which might get me unending legal hassles, which might get me into trouble with the dean, which might get me bad press, which will certainly get me enmity of these powerful companies."* [32]

Mr. Finkelstein provides no evidence to support his suggestion that "these powerful [filtering] companies" intimidate institutions such as Consumer Reports and the Kaiser Family Foundation. To the knowledge of the exemption opponents, no such evidence exists. The exemption opponents are unaware of any filtering company ever taking any sort of action that could even vaguely be described as "intimidating" toward research institutions, nor of any comment by a member of one of these institutions suggesting they felt "intimidated" by filtering companies.

Mr. Tepp observed that the research questions Mr. Finkelstein poses "sound like interesting questions."[33] The exemption opponents do not take issue with Mr. Tepp's observation -- indeed, some of Mr. Finkelstein's observations are "interesting." What we take issue with is that "interesting" is a standard that requires the drastic remedy of circumvention.

No evidence presented to the panel suggests that the broad, vaguely defined activity of exploring "architectural issues" generates research that is considered of important value to the research community and public policy community.

Proponents present two examples of research conducted during the exemption period that purports to require circumvention: the "loophole example" presented by Mr. Finkelstein, and the "sub directory" example presented by Mr. Tyre.

Neither example required circumvention, as is documented below.

The "Loophole Example"

As the exemption opponents showed in both written and oral testimony, there are serious problems with the "loophole example," which is undocumented and the "importance" of rests entirely on inference.

Mr. Finkelstein states factually in his written comments to the panel that:

> *"..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."* [34]

This claim the exemption opponents assert in written comments is disproved by Mr. Finkelstein's own writing, since this information was available on N2H2's website through the N2H2 URLChecker, at the time Mr. Finkelstein published his writing. Mr. Finkelstein admitted as much under oral testimony, stating that:

> *"When I put one of the sites which was listed into the query database that said it was a loophole and it came back and said, "loophole sites," it didn't tell me what a loophole was."* [35]

Mr. Finkelstein was pressed on this point by Mr. Kasunic in oral testimony:

> *MR. KASUNIC: David had said that you could have discovered the loophole category, even without circumvention, but is what you're saying that it's the scope? You could have identified that this existed, but you could have never identified what the scope of that category was?*
>
> *MR. FINKELSTEIN: The extent of it would never have been found by sampling.*[36]

Mr. Finkelstein's "loophole" example is another example of exploring "architectural features." Again, the opponents do not dispute the idea that it is difficult, but by no means impossible, to explore the full extent of "architectural features", such as the "extent" of a category, but do dispute the necessity of such "explorations," or the notion that such "explorations" require the most convenient method available.

As has been previously described, an estimation of the extent of a category can be determined with sampling. For example, the website www.multiproxy.org contains a list of "loophole" proxy servers a researcher could check against the N2H2 database to determine how many of them were categorized by N2H2

Further, Mr. Finkelstein refused to present any evidence to document his claim to have circumvented N2H2's copyright protection. Mr. Finkelstein simply repeated that he was afraid of being sued, so the panel should take his word that he circumvented N2H2's software. As Mr. Kasunic suggested in a question to the panel, there are serious factual problems with claims such as Mr. Finkelstein's:

> *MR KASUNIC…Regarding the burden for continued exemption, which the library associations support here, in your view, must a proponent prove how many will be able to accomplish or have actually accomplished the circumvention during a given period in order to sustain their burden?*[37]

In reality, Mr. Finkelstein's "proof" of circumvention amounts to nothing more than a tautology: he has "proven" he has done something, but cannot provide the proof, therefore the panel should declare his proposition "true." Using this "standard" of proof anyone can claim almost anything to be "true."

The "Subdirectory" Example

Mr. Tyre makes two main arguments as to why existing sampling techniques are inadequate for evaluating filtering database. First, he argues that "URL checkers" are inadequate because not all filtering companies have them. Second, he argues that sampling in general is inadequate because he believes it is difficult to locate individual pages that are blocked in subdirectories of web sites. Both arguments are flawed.

Mr Tyre first asserts that URL checkers are generally inadequate for sampling:

> *So we've got nine major censorware companies, five don't even have them. So let's completely throw them out for purposes of talking about URL checkers. That's half the industry right there.*[38]

As opponents pointed out in their initial comments, URL Checkers are a convenience offered by some vendors, while serious researchers will use an evaluation copy of the software:

> *Nearly all filtering companies allow anyone to download a trial copy of the filtering software and accompanying database for a 30-day evaluation. 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.* [39]

Therefore, the lack of URL Checkers by some vendors is not a serious limitation for researchers seeking to evaluate such filtering database, since they can obtain an evaluation copy.

The second argument Mr. Tyre makes is that querying presents problems with examining classifications made by filtering companies because multiple pages in multiple subdirectories within a website may contain different classifications:

> *And this next set of exhibits is intended to illustrate for any database querying method, not just for N2H2 URL checkers, that there are problems with that can be solved by decrypting, looking at the list, but that cannot be solved effectively simply by database querying…Now you'll see on the first page of Exhibit 5 I called up the site peacefire.org to see how it was classified. And it's classified not currently categorized in the N2H2 database. Great. Peacefire's clean. Don't have to worry about it. Move on to the next domain name, right? Wrong. Turn to the next page. Go to a subdirectory in peacefire.org, peacefire.org/bypass. That subdirectory is blocked by N2H2 as a loophole site…*
>
> *So, what do you do when you build a database for purpose of doing a database inquiry? Do you do it just with domain names? Do you do with directories? Do you do it with subdirectories? How do you build that database and how do you even know what subdirectories that you are to include in the database? This is a problem.*

These examples that I just gave to you came from Seth's decrypted black list which Mr. Burt claims Seth never decrypted. That's how I know about these examples, and it's unlikely I ever could have found them without Seth having decrypted the black list and given me these examples.

MS. PETERS: So you're basically saying that decryption is the only way to have gotten this?
MR. TYRE: Sure. For this purpose, yes… the only way to find blocks at this level of granularity is by doing decryption. [40]

Mr. Tyre is incorrect in his assertion that "the only way to find blocks at this level of granularity is by doing decryption." If Mr. Tyre, or anyone else, wanted to find out if N2H2 rated various pages and subdirectories within a website such as Peacefire.org, there is a relatively straightforward method by which they could do so that does not involve encryption, but rather "spidering" technology.

"Spidering" is well-developed technology used by search engines and other web tools to "spider" through an entire website by following each link on the website, and building an index of each page.

A number of software tools for spidering are widely available on the World Wide Web. One such popular tool is WebWhacker, which is available on line at www.bluesquirrel.com.

Mr. Tyre could have downloaded a copy of Web Whacker, built an index of all the pages on Peacefire.org, then checked each page against N2H2's URL Checker or through a trial version of N2H2. Mr. Tyre could have either done this manually by cut and pasting each URL, or used one of many widely available scripting programs, such as PERL to automate this process.

While the "spidering" method does require some effort and software installation on the part of the researcher, it clearly would accomplish the same goal of evaluating the extent of categorization throughout a specific website or websites without requiring circumvention.

The Record Supports that Trial Versions of Filtering Databases are Available to Researchers

Both Mr. Tyre and Mr. Finkelstein offered extensive comments in the hearings regarding their ability to access trial copies of filtering software.

Mr. Tyre discusses multiple incidents of being allowed to access trial copies from several vendors on repeated occasions, despite the fact that these vendors were fully aware of the fact that Mr. Tyre's purpose was to criticize their software. Mr. Tyre was granted trial copies under such circumstances by three different filtering companies, 8e6 Technologies (maker of X-Stop), SurfControl (maker of Cyber Patrol), and Secure Computing (maker of SmartFilter), as he related in his testimony:

> *…a product called SmartFilter when their sales person after I registered actually called me. And before he called me, he did a search on me and he saw I was a member of the Censorware Project and saw what the Censorware Project did. And he still let me have a sample.*
>
> *In the Mainstream Loudoun case we went through probably 8 or 9 different iterations of X-Stop*
>
> *So we did that a second time. They unblocked it, they reblocked it. I won't tell you exactly how many times we went through this cycle, but eventually I decided to have some fun with this. I wrote an open letter, you know, to the President of CyberPatrol*[41]

Mr. Tyre was asked if he knew of other instances where other researchers were denied access, but only recall the incident described by Mr. Finkelstein:

> *MR. CARSON: Have there been cases where the Censorware Project or people in similar situations have requested access to lists of blocked websites and that access has been refused?*
> *MR. TYRE: Yes.*
> *MR. CARSON: Okay. Give me some idea of the nature and quantity of those attempts?*
> *MR. TYRE: Well, you already have in the record that N2H2 flat out turned down Seth Finkelstein once.*
> *MR. CARSON: Yes, that's once.*
> *MR. TYRE: Once.*
> *MR. CARSON: I'm trying to get a sense of quantity of the problem, the nature of the problem.*
> *MR. TYRE: There was a time when I tried to get one and, honestly, I'm blanking on which product it was. There are so many of them, they sometimes blend together. And they turned me down.*[42]

During his oral testimony, Mr. Finkelstein describes an incident in which he was refused access to a trial copy of N2H2' s database:

> *Further, the last time I tried to get the demo from N2H2, straightforwardly get it filling out my name, I was outright refused. I was worse than outright refused. I was led on, and then I got a really obnoxious e-mail from their salesperson telling I'm just not going to quote it; it was so obnoxious.*[43]

N2H2's records indicate that Mr. Finkelstein was granted a fully functioning trial copy of N2H2's software, including the database on March 24, 2001. After this first 30-day trial expired, Mr. Finkelstein requested and received a second copy of N2H2's software on April 28, 2001. On March 20, 2002 Mr. Finkelstein requested and received a third copy of N2H2's software. After this third trial expired, Mr. Finkelstein requested a fourth free copy N2H2's software, and was refused.

Similar to Mr. Tyre's experience with SmartFilter, X-Stop (8e6 Technologies) and Cyber Patrol (Surfcontrol), N2H2's employees were aware of Mr. Finkelstein's anti-filter research when they provided him free trial copies. Mr. Finkelstein was familiar to N2H2's employees at that time because of his frequent postings to the N2H2 stock investor message board on Yahoo, where Finkelstein regularly issued the recommendation of "Strong Sell" regarding N2H2's stock, referred to those who purchased N2H2 stock as "fools," and posted copies of his anti-filter research critical of N2H2.[44] Like the employees of Surfcontrol, SmartFilter, and 8e6 Technologies, N2H2's employees did not deny free trial copies to anti-filter activists such as Mr. Finkelstein.

N2H2's provision of free software is not absolutely unlimited, as it costs N2H2 time and money to process free trials. Filtering researchers who exhaust the supply of free trials with filtering companies can always purchase a functioning copy of the software, or rely on the URL Checker.

The Threats Posed by the Exemption are Real

Opponents have documented the very real threat of harm from the exemption in the early testimony, particularly the Microsystems case.

There was some confusion among the panel and witnesses about the facts of the Microsystems case. The exemption opponents would like the record to reflect the facts of this case.

Mr. Band made the following assertion in his testimony:

> *Fourth, the reference to the Microsystems case is completely besides the point. That case involved the development of a bypass code that disabled the filter. It had nothing to do with accessing the database for fair use purposes.*[45]

The notion that the Microsystems case "had nothing to do with accessing the database" is refuted by the plain language of the appellate court finding, as cited in the exemption opponent's written testimony:

> *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.*** *[Emphasis added.]*[46]

Finally, the exemption opponents would like to address the issue of actual or potential harm from circumvention.

Exemption opponents pointed out in oral testimony:

> *MR. BURT: If I could just follow up quickly with your question of irreparable harm, in addition to the harm to the security of our product, once our list is available to someone such as Mr. Finkelstein, who has it, are we at that point supposed to just simply assume that he's going to use it responsibly? We have ceded all control over our copyrighted material, over our database, to somebody else, just on the assumption, without any kind of NDA, without any kind of contract, without any agreement, that he is not going to misuse that property; he's not going to sell it to somebody else; he's not going to profit from it. We have no guarantees of that.*[47]

Nothing illustrates the risks of allowing someone like Mr. Finkelstein to circumvent the copyright protection on our database better than Mr. Finkelstein's own behavior during the exemption hearing:

> *MR. FINKELSTEIN: David, will you authorize me to send to the members of the Panel the complete N2H2 blacklist to prove that I have, indeed, circumvented the encryption?*[48]

While the proponents are not convinced Mr. Finkelstein has, in fact decrypted the N2H2 database, if in fact he has, Mr. Finkelstein's spontaneous threat to begin distributing N2H2's decrypted database shows the danger of allowing such decryptions. As the opinion in *Edelman v. N2H2* stated:

> *There is no plausible protected constitutional interest that Edelman can assert that outweighs N2H2's right to protect its copyrighted property from an invasive and destructive trespass.*[49]

Conclusion

Proponents have failed to meet every burden placed upon them by the statue.

Proponents have failed to adequately define a "class of works", as it is very unclear which applications would be covered by their proposed exemptions.

Proponent's main public interest justification for an exemption, the use of mandated filtering software by government agencies, has collapsed in wake of the Supreme Court decision ruling that the use of filtering software in schools is not an abridgement of constitutional liberties.

Proponents have also failed to demonstrate that there is any harm to not allowing an exemption, as there are fully adequate alternative methods for evaluating filtering software available.

Finally and most importantly, proponents have made no documented use of the exemption during the three year period.

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

Footnotes

[1] Testimony of Steve Metalitz, May 14, 2003 Copyright Office Rulemaking Hearing, p. 25.
[2] IDC, "Worldwide Secure Content Management Software Market Forecast and Analysis, 2002–2006: Vendor Views," June 2002.
[3] IDC, "Worldwide Secure Content Management Software Market Forecast and Analysis, 2002–2006: Vendor Views," June 2002.
[4] IDC, "Worldwide Secure Content Management Software Market Forecast and Analysis, 2002–2006: Vendor Views," June 2002. Table 1.
[5] Symantec website, visited June 25, 2003. Available at http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=133&EID=0
[6] Trend Micro website, visited June 25, 2003. Available at http://www.trendmicro.com/en/products/gateway/iswm/evaluate/overview.htm
[7] Network Associates website, visited June 25, 2003. Available at http://www.mcafeeb2b.com/common/media/mcafeeb2b/us/products/pdf/ds_us_webshield_appliances.pdf
[8] Computer Associates website, visited June 25, 2003. Available at http://www3.ca.com/Solutions/Overview.asp?ID=163&TYPE=S
[9] NetIQ website, visited June 25, 2003. Available at http://www.webmarshall.com/webmarshal/withN2H2.asp/MSASP/REFID.MARSHAL/MSASP.HTML
[10] Websense press release, June 5, 2003. Available at http://www.websense.com/company/news/pr/03/060503.cfm
[11] Surfcontrol website, visited June 25, 2003. Available at http://www.surfcontrol.com/products/total_filtering.aspx
[12] IDC, "Worldwide Secure Content Management Software Market Forecast and Analysis, 2002–2006: Vendor Views," June 2002. Table 1.
[13] Bsafe Online website, "Bsafe Home", visited June 26, 2003. Available at http://bsafehome.com/about.asp?a=future
[14] Testimony of James Tyre, May 14, 2003 Copyright Office Rulemaking Hearing, p. 8.
[15] ALA v. U.S., Available at http://www.supremecourtus.gov/opinions/02pdf/02-361.pdf
[16] Testimony of James Tyre, May 14, 2003 Copyright Office Rulemaking Hearing, p. 8.
[17] Testimony of Jonathan Band and Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 86-87.
[18] "Ruling ignites libraries' push to end secrecy of Net filters," Associated Press, June 25, 2003. Available at http://seattletimes.nwsource.com/html/businesstechnology/135076082_onlinepornfilters25.html
[19] BioNet website, visited June 25, 2003. Available at http://www.netnanny.com/products/netnanny5/cipa.html
[20] Stone, Glenn, "Necessary Censorship: Web Filtering with Open Source," Linux Journal, April 16, 2003. Available at http://www.linuxjournal.com/article.php?sid=6807
[21] SquidGuard website, visited June 25, 2003. Available at http://www.squidguard.org/blacklist/
[22] Dansguardian.org website, visited June 25, 2003. Available at http://dansguardian.org/?page=introduction
[23] Murdock, Cindy. "Open Source Filtering," School Forge, April, 2003. Available at http://opensourceschools.org/article.php?story=20030401120601397
[24] FCC Federal-State Joint Board on Universal Service, Children's Internet Protection Act, April 5, 2001. Available at http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc
[25] Testimony of Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 38
[26] Testimony of Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 86
[27] Testimony of James Tyre, May 14, 2003 Copyright Office Rulemaking Hearing, p. 7
[28] Sims, Michael. Censorware.org, visited June 25, 2003. Available at http://censorware.org
[29] Testimony of James Tyre, May 14, 2003 Copyright Office Rulemaking Hearing, p. 60.
[30] Censorware Project, "Passing Porn, Banning the Bible: N2H2's Bess in public schools," visited June 25, 2003. Available at http://censorware.net/reports/bess/

[31] The report is undated, but states " N2H2 is also now planning a stock offering scheduled for the end of July, 1999," indicating it was written prior to July, 1999.
[32] Testimony of Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 78
[33] Testimony of Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 78
[34] Comment 33, Seth Finkelstein
[35] Testimony of Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 36
[36] Testimony of Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 55
[37] Testimony of Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 72
[38] Testimony of James Tyre, May 14, 2003 Copyright Office Rulemaking Hearing, p. 28
[39] Reply Comments 11, Opponents, page
[40] Testimony of James Tyre, May 14, 2003 Copyright Office Rulemaking Hearing, p. 33-38
[41] Testimony of James Tyre, May 14, 2003 Copyright Office Rulemaking Hearing, p. 40-42
[42] Testimony of James Tyre, May 14, 2003 Copyright Office Rulemaking Hearing, p. 54-55
[43] Testimony of Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 48
[44] Yahoo Message Board, visited June 26, 2203. Available at http://messages.yahoo.com/?action=q&board=NTWO . Mr. Finkelstein recommended a "Strong Sell" of N2H2's stock on 03/05/02, 02/26/02, 11/30/01, 10/05/01, 9/23/01, 9/05/01, 9/04/01, 8/14/01, and 8/13/01. On 02/26/02 he posted a message titled "Greater-fool theory", available at http://messages.yahoo.com/bbs?.mm=FN&action=m&board=22689355&tid=ntwo&sid=22689355&mid=1658
[45] Testimony of Jonathan Band, April 11, 2003 Copyright Office Rulemaking Hearing, p. 72
[46] R11, p. 36, citing Microsystems Software, Inc. v. Scandinavia Online, 226 F.3d 35 (1st Cir. 2000).
[47] Testimony of David Burt, April 11, 2003 Copyright Office Rulemaking Hearing, p. 64
[48] Testimony of Seth Finkelstein, April 11, 2003 Copyright Office Rulemaking Hearing, p. 89
[49] Testimony of David Burt, April 11, 2003 Copyright Office Rulemaking Hearing, p. 20, citing Edelman v. N2H2.