UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MICROSYSTEMS SOFTWARE, INC. Plaintiff, v. SCANDINAVIA ONLINE AB, ISLANDNET.COM, EDDY L.O. JANSSON, and MATTHEW SKALA Defendants.	CIVIL ACTION NO. 00-10488-EFH

OPPOSITION TO MOTION FOR PRELIMINARY INJUNCTION

Nonparties Waldo L. Jaquith, Lindsay Haisley, and Bennett Haselton (the "Nonparties") hereby respectfully request that this Court deny the motion for preliminary injunction sought by plaintiff Microsystems Software, Inc. ("plaintiff" or "Microsystems"). In the alternative, the Nonparties request that the Court declare that the TRO previously entered, and any Preliminary Injunction that the Court may hereafter enter, does not apply to or bind the Nonparties.[1]

This case, which is premised on a flawed reading of U.S. copyright law, is a thinly-veiled attempt to stifle legitimate examination and criticism of a controversial Internet filtering product. Plaintiffs are asking the Court to grant an injunction that is not necessary (because plaintiffs themselves can prevent virtually all of the harm they allege without the need for a court order) and is improper.

[1] The within motion is filed without waiver of the Nonparties' position that they are not subject to the personal jurisdiction of this Court. The Nonparties do not concede that this Court has jurisdiction over them and do not waive any defenses provided by Rule 12(b)(1), 12(b)(6) or on any other basis.

Procedural Background

On March 17, 2000, plaintiffs sought and obtained an ex-parte temporary restraining order (the "TRO") that is directed against defendants who reside in Sweden and Canada. That order expires at the hearing on Monday, March 27, 2000, at which time plaintiffs apparently intend to request that it be converted into a preliminary injunction.

This motion is filed on behalf of three individuals who are not named as defendants but two of whom have been served by plaintiff's counsel by electronic mail ("e-mail") with a copy of the TRO and a message implying that they are bound by the order.[2]

The Nonparties maintained "mirror" web pages that included certain computer programs. For at least some of the Nonparties, their "mirror" page contained those programs collectively — along with an essay containing political and social commentary on censorship software — in a file called "CP4break.zip." Plaintiff apparently contends that the content of these mirror sites is subject to the TRO. "Mirror" sites are Internet web pages or sites that contain an exact copy of some other site or page. Thus, the Nonparties placed copies of the web pages of the defendants, about which plaintiffs complain, on the Nonparties' web sites.

The Nonparties respectfully oppose extension of the TRO or entry of any comparable preliminary injunction. Alternatively, the Nonparties request clarification from the Court that they are not bound by the TRO or by any subsequent preliminary injunction. Although the Nonparties do not believe that they are so bound, plaintiffs have taken the position that they are and accordingly the Nonparties are placed in a precarious position absent clarification from the Court of their rights and/or obligations.

---

[2] The third Nonparty will presumably be served shortly or will have been served by the time of the hearing. The Nonparties have standing to file the within opposition to the preliminary injunction because plaintiffs have expressly asserted that the injunction would apply to the nonparties, and have sought to serve them with the underlying TRO order and a related subpoena. (See also Motion to Quash Subpoenas, filed herewith.) In the alternative, the

Factual Background

Plaintiff is the corporate owner of a product known as Cyber Patrol. Cyber Patrol is a product designed to prohibit its users from obtaining access to designated Internet web sites. Cyber Patrol has staff who supposedly examine some or all of the approximately 1 billion web pages in existence.[3] The staff makes a judgment (or delegates that judgment to a machine or program) that the content of a particular page is or is not acceptable according to a pre-determined set of guidelines. If the content violates the guidelines, it is placed on a list of sites that cannot be accessed when Cyber Patrol is running on a particular computer. For example, if the page shows nudity or information about gambling, Cyber Patrol's staff might put the page on its list of blocked sites. Thereafter, users of the product who attempt to access the page are prevented from doing so. Users of the blocked list sites frequently obtain, as part of a subscription service, an updated program containing newly blocked sites.

Cyber Patrol was originally designed for use by parents to prevent the children in their home from accessing sites that the parents found objectionable. It has since been purchased and used by public entities such as libraries, universities, corporations, and schools.

The value of products such as Cyber Patrol has been a matter of significant public debate for years. The Supreme Court referred to such products as a useful alternative to criminal laws in Reno v. ACLU, 521 U.S. 844 (1997). In other contexts, however — for example, in public libraries — the use of such products has been found unconstitutional. Mainstream Loudoun v. Board of Trustees, 2 F. Supp. 2d 783 (E.D. Va. 1998); 24 F. Supp. 2d 552 (1998). There was a recent public vote in Holland, Michigan about the wisdom of installing such products in the

---

Nonparties should at least be entitled to the protection of an order declaring that they are not in fact governed by the terms of the TRO or of any preliminary injunction the Court might enter.

[3] Clearly it is impossible for all such sites to be examined in person. Accordingly, the software undoubtedly uses various imperfect automated screening devices to make its selection of which sites to block. The nature and identity

public libraries. (The community voted against the product. "Library Net filter proposal defeated," USAToday, Feb. 23, 2000; Keith Bradsher, "Town Rejects Bid to Curb Library's Internet Access," New York Times, Feb 23, 2000, at A12.) Legislation has been introduced in Congress and in the states requiring the use of such products in libraries and schools.

There have been numerous articles in the press about products such as Cyber Patrol. Many have been favorable, explaining their value for parents. Others have been harshly critical, arguing that such products inevitably heavily overblock and underblock. The manufacturers of blocking products generally admit that the products often block sites that no one believes meet the criteria for blocking and they often fail to block sites that do meet the criteria. The program in Loudoun, for example, blocked the site of the American Association of University Women, Maryland chapter. It also blocked a map of Disney World.

Cyber Patrol and most, though not all similar products, keep the list of sites they block a secret from those who purchase the product, those who are considering purchase of the product, and the public. Thus, owners and prospective owners have no method of properly evaluating the value of the product. Further, public officials who use the product end up blocking library patrons from accessing sites even though the officials do not know what they have blocked. Critics may find examples of overblocked sites or underblocked sites by random accident or trial and error. They may not view the list of blocked sites to show the adequacy or inadequacy of the product or to compare its value with its competitors. The updated program received by owners containing newly blocked sites is also secret.

Plaintiffs sued two defendants, one who resides in Sweden and one who resides in Canada. Plaintiffs assert that, in Sweden and/or in Canada, defendants obtained a copy of Cyber Patrol. Plaintiffs admit that they do not know the method by which defendants

---

of which sites are thereby blocked has become a matter of great public debate in the Internet community, the

obtained that copy. Plaintiff argues that defendants ran the Cyber Patrol program in order to create an add-on program that could circumvent the portions of it that Cyber Patrol wants to keep secret. By engaging in the process of what some call "reverse engineering" in order to determine how the program works, the person engaging in the "reverse engineering" inevitably creates a so-called "intermediate copy" of the software, and places such a copy, at least temporarily, in the "random-access memory" ("RAM") of the computer he or she is using. It is this creation — in Sweden and/or Canada — of one or more "intermediate copies" of the Cyber Patrol software that plaintiff apparently contends is a violation of the U.S. Copyright Act.

The Nonparties do not concede the accuracy of any of the facts alleged in the Complaint. However, accepting the allegations as true, the only allegation of a violation of copyright concerns activity that occurred entirely outside the United States.

Again accepting the allegations as true *arguendo*, it would appear that defendants used their own ingenuity to discover a method by which they could determine the list of web sites that are blocked by Cyber Patrol. They wrote an article explaining how they did this and how another person could do the same thing. The article has not been the subject of this action and remains on the web in multiple copies. People can use it to re-create the defendants' program. (As noted, for some mirror sites, the article is one of the constituents of the cp4break.zip file that plaintiff apparently believes must be deleted from the web everywhere it appears.) Defendants also apparently wrote their own computer program that, if downloaded, would allow someone who already owns a legal copy of Cyber Patrol to view the entire list of blocked sites. The program is of no value to, and has no impact on, anyone who doesn't already own a copy of Cyber Patrol.

---

education community, and the civil liberties community in recent years. See infra.

Accordingly, it does not substitute for or compete with Cyber Patrol in the marketplace. It is this program which is the subject of the TRO and the requested preliminary injunction. Thus, the TRO — and the Preliminary Injunction now sought by plaintiff — would not do what a copyright injunction is normally designed to do, namely restrain the illegal duplication or distribution of a plaintiff's own copyright-protected material. Rather, such orders would prohibit the dissemination of original works of authorship, of significant political and social dimension, which do not contain a copy of anyone else's copyrighted work (but which, plaintiffs argue, can be used to defeat their efforts to keep some portion of their product secret).

Plaintiff, moreover, concedes that it can fix its software so that defendants' code will no longer work to "crack" the Cyber Patrol code. Indeed it has apparently done so. It has also, apparently (and easily could if it has not yet done so) added to its list of "blocked" web sites each and every "mirror" site (such as the ones until recently maintained by the Nonparties). Cyber Patrol has taken this approach in the past. For example, it has previously blocked the web site, "peacefire.org", of Bennett Haselton, one of the Nonparties. Plaintiff's theory that children will obtain access to the decryption software by accessing it on a web site and will use it to deactivate their parents' attempts to limit their access to certain web sites thus makes no logical sense. As long as the web pages that include the defendants' program are blocked by Cyber Patrol, no child whose parent is using an updated version of Cyber Patrol will be able to access that program.[4]

The defendants' program also allows a user to view the password selected by a Cyber Patrol user. The primary owner of Cyber Patrol (frequently, though not always a parent) is given a name and password. With this name and password, the primary owner can turn the product on

or off and, within limits, customize it. Cyber Patrol promotes its product by relying heavily on the value of this password system. The program written by defendants illustrates that users should not take comfort from the Cyber Patrol's use of this system, which is only weakly hidden. Moreover, as noted above, defendants' software cannot be accessed to circumvent Cyber Patrol if plaintiff simply adds to its list of blocked sites the ones on which the said software is contained. That is a simple and technologically-available solution that does not require this Court to take the extreme step of entering an order that would constitute a prior restraint on speech having a significant social and political dimension.

Finally, there is no allegation that defendants created this original work for commercial profit. They apparently did so to advance human knowledge about the weakness of computer programs designed to block or censor web access. Defendants have sparked and contributed to the ongoing public debate over the adequacy of the method by which this particular product has hidden material it wants to hide. The Nonparties created mirror sites to make the same points and also as a commentary on their disapproval of plaintiff's efforts to use the courts to censor speech.

Mirror sites of the disputed program now exist on many sites on the web, some of which are unquestionably outside the jurisdiction of this Court. Thus, the Court's order would not prevent the distribution of the defendants' program. It would succeed only in constituting an unusual, unwarranted, and unnecessary prior restraint on free speech. It would do so, moreover, in a context in which the court lacks both subject matter and personal jurisdiction. The preliminary injunction sought by plaintiff cannot and should not enter.

---

[4] Failure to use the latest version of the Cyber Patrol software makes the software essentially ineffective anyhow

ARGUMENT

I. THE COURT LACKS PERSONAL OR SUBJECT-MATTER JURISDICTION

Before reaching any substantive issues in this case, the Court is bound to examine whether it has subject matter jurisdiction over the claim presented and personal jurisdiction over the defendants. It has neither.

A. Subject-Matter Jurisdiction

The gravamen of plaintiff's complaint, and the basis for its injunction motion, is a claim of copyright infringement. Plaintiffs allege that defendants made "intermediate copies" of plaintiff's copyright-protected software. But plaintiffs do not, and cannot, claim that the software that defendant created and posted on the Internet contains an infringing copy of plaintiff's software. Rather, their claim is that in the course of developing their software, the "reverse-engineering" process used by defendants required them to make intermediate copies of the plaintiff's program.

Unfortunately for plaintiff's case, the Copyright Act does not govern copying that occurs in another country. Plaintiff's complaint alleges that defendants Jansson and Skala engaged in reverse engineering of plaintiffs' copyrighted Cyber Patrol program in knowing and willful violation of U.S. copyright law. All of the acts of reverse engineering alleged in plaintiffs' complaint, however, occurred in Canada or Sweden. It is well-settled that U.S. Copyright laws have no extraterritorial application. E.g., Twin Books Corp v. Walt Disney Co, 83 F.3d 1162, 1166-67 (9th Cir. 1996); Update Art v. Modlin Publications, 843 F.2d 67, 73 (2d Cir. 1988). See United Dictionary v. G&C Merriam Co., 208 U.S. 260 (1908). "Because the copyright laws do not apply extraterritorially, each of the rights conferred under the five section 106 categories must be read as extending 'no farther than the [United States'] borders." Subafilms, Ltd. v.

---

since new web pages of the sort that Cyber Patrol deems objectionable are created literally on a daily basis.

MGM-Pathe Communications Co., 24 F.3d 1088, 1094 (9th Cir. 1994) (en banc) (quoting 2 Paul Goldstein, Copyright: Principles, Law and Practice § 16.0 at 675 (1989)).[5]

The sole activity alleged to have occurred in the U.S. is that defendants "bragged about their unlawful conduct in a March 11, 2000 press release that they circulated widely on the Internet, including through web sites in Massachusetts and elsewhere in the United States." Circulating a press release describing reverse engineering, even if the reverse engineering were itself unlawful, does not and could not violate U.S. copyright law.[6]

B. Personal Jurisdiction

A second threshold obstacle to plaintiff's pursuit of this case is the lack of personal jurisdiction over the defendants. There are two forms of jurisdiction that a plaintiff might assert when attempting to bring a nonresident into a federal (or state) court in Massachusetts: general jurisdiction or specific jurisdiction. See Foster-Miller, Inc. v. Babcock & Wilcox Canada, 46 F.3d 138, 144 (1st Cir. 1995). "Specific jurisdiction exists where 'the cause of action arises directly out of, or relates to, the defendant's forum-based contacts." E.g. Fairview Mach. & Tool Co. v. Oakbrook Int'l, Inc., 56 F. Supp. 2d 134, 137 (D. Mass. 1999). General jurisdiction exists for any cause of action if "the defendant has engaged in continuous and systematic activity, unrelated to the suit, in the forum state." Foster-Miller, 46 F.3d at 144.

[5] Although some courts have permitted the award of damages for events outside of the United States that resulted from infringing acts committed within the United States, see, e.g., Update Art, 843 F.2d at 73, if the infringing acts occur beyond U.S. borders, there is no violation of Title 17 of the U.S. Code. Subafilms, 24 F.3d at 1094-96.

[6] Plaintiff's complaint alleges in counts III, IV, V and VI that the named defendants' acts of reverse engineering violate the tort and contract law of some unspecified state. These claims are presumably included in an attempt to persuade this court to exercise jurisdiction over this dispute, despite the fact that defendants' alleged acts are beyond the reach of U.S. copyright law. The United States, Canada and Sweden are all signatories to the Berne Convention for the Protection of Literary and Artistic Works. The Treaty affords international copyright protection by permitting citizens of each signatory nation to claim "national treatment" under foreign nation's copyright laws. Under the Berne Convention, Microsystems is entitled to the benefit of Canadian and Swedish copyright protection in Canadian and Swedish courts. The Treaty does not entitle US citizens to seek recourse for extraterritorial infringement by subjecting foreign nations to liability for extraterritorial acts — whether the source of liability is federal copyright law or the common or statutory law of a state. Subafilms, 24 F.3d at 1097. Further, the exercise of the Court's diversity jurisdiction is doubtful given that there has been no evidence of the jurisdictional threshold being met.

Neither form of personal jurisdiction applies here — either to the original defendants, or, for that matter, to the Nonparties filing the within papers. None of these persons lives or works in Massachusetts, operates any business in Massachusetts, sells products in Massachusetts, or engages in any other "continuous and systematic activity" in Massachusetts. There is neither allegation nor evidence supporting any theory that plaintiffs might advance suggesting that the defendants have any such minimum contacts either. Accordingly, general jurisdiction does not apply. Nor does specific jurisdiction, since the copyright claim does not arise out of any conduct taken by any defendant in Massachusetts. Indeed, there is no allegation that any defendant ever set foot in Massachusetts, engaged in any copying in Massachusetts, or bought or sold any product in Massachusetts.

That the defendants' software may have been made available over the Internet in Massachusetts (as in every other state and industrialized country of the world) merely by virtue of having been posted on defendants' web sites does not give rise to personal jurisdiction in Massachusetts. Of course, the defendants have not committed copyright infringement over the Internet — they have not, for example, posted an unauthorized copy of Plaintiffs' software on a web-site accessible in Massachusetts. That might make this a closer case, although even then personal jurisdiction should not be found. Cf. Digital Equip. Corp. v. Altavista Tech., Inc., 960 F. Supp. 456, 463 (D. Mass. 1997). Rather, the allegation is simply that by engaging in copyright infringement in Sweden or Canada, defendants created a product that was then posted on the Internet.

A second factor of note is that defendants are not selling or making any other commercial use of their software. Rather, it is being provided as a political and social comment on an issue of significance to the Internet, education, and civil liberties communities.

Where the sole allegation is that an allegedly infringing work has been made available over the Internet to every state and country in the world, the courts have repeatedly rejected the notion that personal jurisdiction is therefore available in any state in which plaintiff is located and/or chooses to sue. See, e.g., Millenium Enterprises, Inc. v. Millenium Music, LP, 33 F. Supp. 2d 907, 915 (D. Or. 1999) (explaining that the situation "at the opposite end" from any possibility of a finding of personal jurisdiction is one where — as here — "a defendant simply posts information on a Web site which is accessible to users in the forum state as well as others"). See also Zippo Manuf. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123 (W.D. Pa. 1997); ESAB Group, Inc. v. Centricut, LLC, 34 F. Supp. 2d 323 (D.S.C. 1999); Edberg v. Neogen, 17 F. Supp. 2d 104 (D. Conn. 1998). Where, as here, the defendants are not even using their web sites for commercial or competitive purposes but rather for the advancement of human thought and knowledge and political commentary on the social impact of plaintiffs' products, the argument for personal jurisdiction in this forum is even weaker.

II. PLAINTIFF CANNOT MEET THE INJUNCTION STANDARDS

In order to succeed on a preliminary injunction motion, plaintiff bears the burden of showing that (1) it has a likelihood of success on the merits, (2) there exists, absent the injunction, a significant risk of irreparable harm, (3) the balance of hardships tilts in its favor, and (4) granting the injunction will not adversely affect the public interest. See Concrete Machinery Co. v. Classic Lawn Ornaments, 843 F.2d 600, 611 (1st Cir. 1988) (copyright case). Microsystems cannot meet this burden.

A. Likelihood of Success

Plaintiff cannot succeed on the merits for at least four independent reasons: (1) The Copyright Act does not cover conduct of the sort that plaintiff alleges defendants engaged in,

because it took place outside the United States and the Copyright Act does not have extraterritorial application. (See Part I.A above.) (2) The court lacks personal jurisdiction over the defendants, requiring that the case be dismissed. (See Part I. B above.) (3) The case is moot and must be dismissed for that reason as well. As explained in the Facts section above, plaintiff's claims are moot for two reasons. First, plaintiffs can (and have) patched the software to make defendants' software unworkable. At least as to anyone who has the patch (which anyone can easily obtain), the "key" no longer fits the "lock." Second, since Cyber Patrol blocks (or can block) access to the web sites on which defendants' product is made available, no child who is using a computer on which Cyber Patrol is installed (and properly updated[7]) can get access to the decryption software. (4) Fourth, "reverse-engineering" of software is "fair use," a statutory exception to the Copyright Act. 17 U.S.C. sec. 107.

Even if U.S. copyright law applied (which it does not) plaintiffs would not be likely to succeed in an argument that the Fair Use doctrine would not apply. Federal courts have repeatedly found the reverse-engineering of software to be "fair use," when it is necessary to gain access to the unprotected ideas and processes embodied in source code. See, e.g., Sony v. Connectix, __ F.3d __, 53 U.S.P.Q.2d (BNA) 1705 (9th Cir. 2000); Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992); Atari Games Corp. v. Nintendo of Am. Inc., 975 F.2d 832 (Fed. Cir. 1992).[8] These courts found fair use even though the alleged infringer did so for commercial purposes.

Finally, even if plaintiffs could somehow prevail against the defendants on each of the above four independent obstacles, they cannot show that the mirror sites posted by the Nonparties are copyright infringements, because hosting a mirror site does not require one to

[7] Of course, if the software is not updated, then the same child will have access to all sorts of "objectionable" content since the Web is updated with new sites constantly.

actually reproduce or distribute plaintiffs' software — it merely requires one to copy defendants' software. Absent an allegation, and evidence, that the Nonparties themselves reproduced or distributed Cyber Patrol in the United States, there can be no copyright claim against them. These parties, moreover, cannot be deemed, and have not been shown, to be "acting in concert" with the defendants so as to be encompassed within the scope of the TRO.[9] Accordingly, even if the Court could somehow enter a Preliminary Injunction despite the above obstacles, it should not apply to the Nonparties.

B. Irreparable Harm/Balance of Harms

Even if plaintiffs could show a likelihood of success on the merits, which they cannot, the balance of hardships favors denying the injunction. First, as noted above the defendants' program is useful only to owners of Cyber Patrol. Plaintiffs have the ability to block any Cyber Patrol owner from accessing any web site or page on which the program appears. Thus, they do not need the Court's assistance in obtaining the relief they seek.

It is true that someone could go to a computer that does not have Cyber Patrol, find defendants' site, access the defendants' code, take it back to a computer that does have Cyber Patrol (and that has not added any improvements that defeats the defendants' code) and use the software. Such a person, however, by having access to a computer without Cyber Patrol, already has the ability to defeat all of Cyber Patrol's blocks anyway.

In addition, Cyber Patrol's ability to add the defendants' pages (and similar pages) to their blocked list is likely to be more effective than the Court's order. The defendants' code has now been mirrored by dozens or more other sites, some of which are undoubtedly outside the

[8] The Atari court carved out an exception to this rule where the original copyright-protected work had been obtained by fraud. There is no such allegation (or evidence) here.

[9] One court has defined "acting in concert" as one who "solicits, requests, commands, importunes or intentionally aids such person to engage in such conduct." Estrada v. Senkowski, 1999 U.S. Dist. Lexis 17946 (S.D.N.Y. 1999).

effective control of this Court. Thus, the Cyber Patrol blocking system is likely to be more effective than this Court's orders.

The injunction plaintiffs seek would enjoin the publication of an original, non-infringing work. As such, this is a classic prior restraint on speech. The "chief purpose of the First Amendment is to prevent previous restraints upon publication." Near v. Minnesota, 283 U.S. 697, 713 (1931) (striking down statute that permitted a perpetual injunction against a "malicious, scandalous and defamatory newspaper, magazine or other periodical"). "[A]ny system of prior restraints of expression comes to [the court] bearing a heavy presumption against its constitutional validity." Bantam Books v. Sullivan, 372 U.S. 58, 70 (1963) (morality commission, whose purpose was to recommend prosecution of obscenity, imposed unconstitutional prior restraint by sending notices to booksellers that certain books were objectionable). The Supreme Court has warned that "[e]ven where questions of allegedly urgent national security, or competing constitutional interests, are concerned, we have imposed this most extraordinary remed[y] only where the evil that would result from the reportage is both great and certain and cannot be militated by less intrusive measures." CBS Inc. v. Davis, 510 U.S.1315, 1317 (citing Bantam to stay injunction by South Dakota state court that would have prevented CBS from airing investigative news footage on meat packing industry).

It cannot be disputed that a prior restraint of speech is, itself, irreparable harm to the defendants, the Nonparties, and others. As the Supreme Court has stated, "the loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." Elrod v. Burns, 427 U.S. 347, 373 (1976).

The value of the Nonparties' speech should be obvious. First, as noted, a prior restraint of original speech comes with a very heavy presumption prohibiting its suppression. Second, the

---

There has been no such showing here as to the Nonparties. Creation of a mirror site is not the same as participating

speech has obvious value in enabling owners of the product, prospective owners, and those concerned with the issues raised by the product to engage in a more accurate debate about the merits of it. Owners can determine if the product is so imperfect that they do not wish to use it, or not. Public debate about an important public issue is advanced by the disclosure of the Cyber Patrol blocked list.

The only potential harm to plaintiffs is that for a period of time they might lose some competitive advantage. Competitors could use the public nature of the blocked sites list to make sure that their list includes all pages on Cyber Patrol's list and the additional pages the competitor identified. First, that competitive disadvantage already has occurred since the code was available to the public prior to the TRO. Second, it will not continue. CyberPatrol has now presumably fixed the product so that the code no longer works and newly added blocked sites cannot be seen by owners of the product whether competitors or not. Third, if the Court refuses to grant the preliminary injunction for Cyber Patrol, it can be expected that researchers will examine the security systems of competitors. If their products are as easily defeated, their lists will too be made public. If all of the lists were made public, public debate would be enriched. If some lists were not made public because the product did a better job of hiding the list (making it difficult to create a program to read the list), then maybe that product should obtain a competitive advantage because it has been better engineered.

C. Granting the Injunction Would Adversely Affect the Public Interest.

There is at present a great public debate over the effectiveness, utility, and wisdom of what some call "filtering" or "blocking" software and what others more critically call "censorware." What is clear, however, is that the debate over this issue, like the debate over

---

in the original copying that occurred in Sweden or Canada.

every other social and political issue, must under the First Amendment be open and robust. Defendants' article and software is a contribution to that debate. Some may agree, some may disagree, and some may even be offended by defendants' approach. But their right to express their ideas and disseminate their creative expression (including software) without governmental censorship should not be questioned, particularly inasmuch as the software itself is not an infringement of plaintiff's copyright.

Conclusion

This case presents numerous issues of jurisdiction and law. At bottom, however, it is a case of a corporation seeking a prior restraint of original non-infringing speech about matters of enormous public interest. And, the corporation is doing so even though it has the ability on its own to better cure problems, if any, caused by defendants' actions (by adding defendants' and other sites to the new blocked list and by fixing the product). Plaintiff's request for a preliminary injunction (and/or extension of the TRO) should be denied. In the alternative, at a minimum, the Court should declare that it does not apply to the Nonparties and their "mirror" sites.

Respectfully submitted,

WALDO L. JAQUITH,
LINDSAY HAISLEY, and
BENNETT HASELTON

By their counsel,

_____

Dated: March 24, 2000

Sarah R. Wunsch, BBO # 548767
American Civil Liberties Union of Massachusetts
99 Chauncy Street, Suite 310
Boston, Massachusetts 02111
(617) 482-3170, ext. 323

Christopher A. Hansen
American Civil Liberties Union
125 Broad Street - 18th floor
New York City, New York 10004
(212) 549-2606

Of counsel:
David L. Sobel
Electronic Privacy Information Center
666 Pennsylvania Ave., SE, Suite 301
Washington D.C. 20003
(202) 544-9240

Jessica Litman
Visiting Professor of Law
New York University
40 Washington Square South
New York, NY 10012
(212) 998-6398

Certificate of Service

I hereby certify that on March 24, 2000, I caused a true copy of the above document to be sent to counsel for plaintiff by hand.

_____

Sarah R. Wunsch