

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

MICROSYSTEMS SOFTWARE, INC.

Plaintiff-appellee,

v.

SCANDINAVIA ONLINE AB,
EDDY L.O. JANSSON, and

ISLANDNET.COM,
MATTHEW SKALA

WALDO JAQUITH; LINDSAY

Defendants-appellees
HAISLEY; BENNETT HASELTON

Appellants

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

BRIEF OF APPELLANTS

Of counsel:
David L. Sobel
Electronic Privacy Information Center
1718 Connecticut Avenue, Suite 200
Washington D.C. 20009
(202) 483-1140

Christopher A. Hansen
ACLU Foundation
125 Broad Street - 18th floor
New York City, New York 10004
(212) 549-2606

Jessica Litman
Professor of Law
Wayne State University
468 West Ferry Mall
Detroit, Michigan 48202
(313) 577-3952

Sarah R. Wunsch
Court of Appeals #28628
ACLU of Massachusetts
99 Chauncy Street, Suite 310
Boston, Massachusetts 02111
(617) 482-3170, ext. 323

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES	iii
----------------------------	-----

REASONS WHY ORAL ARGUMENT SHOULD BE HEARD	1
JURISDICTIONAL STATEMENT	1
ISSUES PRESENTED	2
STATEMENT OF THE CASE AND STATEMENT OF FACTS	3
SUMMARY OF ARGUMENT	12
ARGUMENT	15
I. THE COURT SHOULD REVIEW THE ISSUES IN THIS CASE DE NOVO.	15
II. APPELLANTS HAVE STANDING TO APPEAL.	15
III. THE DISTRICT COURT’S REFUSAL TO DETERMINE THE APPLICABILITY OF ITS ORDER TO APPELLANTS AND ITS CONCLUSION THAT APPELLANTS, EVEN IF FOUND TO BE BOUND BY THE ORDER, MAY NOT CHALLENGE ITS LEGALITY, VIOLATED DUE PROCESS.	20
A. The District Court Erred in Refusing To Tell Appellants If The Order Applied to Them or Not.	20
B. The District Court Erred in Holding That Persons Who May Be Bound By An Order and Who Promptly Seek to Contest The Validity of That Order May Not Ever Do So.	23
IV. THE DISTRICT COURT DID NOT HAVE JURISDICTION TO ENTER THE STIPULATED PERMANENT INJUNCTION.	34
V. EVEN IF THE COURT HAD SUBJECT MATTER JURISDICTION, THE U.S. COPYRIGHT LAW WOULD HAVE PERMITTED JANSSON/SKALA TO MAKE A COPY OF CYBER PATROL UNDER THESE CIRCUMSTANCES.	39
A. Fair Use	39
B. License Agreement	49
CONCLUSION	51
CERTIFICATE OF COMPLIANCE	52
CERTIFICATE OF SERVICE	53
ADDENDUM	Add. p. 1

TABLE OF AUTHORITIES

Page

<u>Alemite Manufacturing v. Staff,</u> 42 F.2d 832 (2 nd Cir. 1930)	23
<u>American Geophysical Union v. Texaco, Inc.,</u> 60 F.3d 913 (2 ^d Cir. 1995)	44, 48
<u>Atari Games Corp. v. Nintendo of Am., Inc.,</u> 975 F.2d 832 (Fed. Cir. 1992)	41
<u>Binker v. Pennsylvania,</u> 977 F.2d 738 (3 rd Cir. 1992)	17
<u>Campbell v. Acuff-Rose Music, Inc.,</u> 510 U.S. 569 (1994)	45, 47
<u>Caplan v. Braverman & Kaskey,</u> 68 F.3d 828 (3 rd Cir. 1995)	17, 18
<u>Chase National Bank v. City of Norwalk,</u> 291 U.S. 431 (1934)	23
<u>City Council v. Taxpayers for Vincent,</u> 466 U.S. 789 (1984)	18
<u>Cf. Green Book Int’l v. Inunity Corp,</u> 2 F. Supp. 2d 112 (D. Mass. 1998)	50
<u>Curtis v. City of Des Moines,</u> 995 F.2d 125 (8 th Cir. 1993)	17, 18, 20
<u>Dopp v. HTP,</u> 947 F.2d 506 (1 st Cir. 1991)	16, 20
<u>Elrod v. Burns,</u> 427 U.S. 347 (1976)	26
<u>Fantasy Book Shop, Inc. v. City of Boston,</u> 652 F.2d 1115 (1 st Cir.1981)	24
<u>Felzen v. Andreas,</u> 134 F.3d 873 (7 th Cir. 1998 aff’d sub nom <u>California Pub. Employees</u> <u>v. Felzen</u> , 525 U.S. 315 (1999)(per curium)	19
<u>Freedman v. Maryland,</u> 380 U.S. 51(1965)	24

<u>G & C. Merriam v. Webster,</u> 639 F.2d 29 (1 st Cir. 1980)	19, 23, 24
<u>Grayned v. City of Rockford,</u> 408 U.S. 104 (1972)	22
<u>Hansberry v. Lee,</u> 311 U.S. 32 (1940)	23
<u>Harper & Row Publishers, Inc. v. Nation Enterprises,</u> 471 U.S. 539 (1985)	44, 45, 48
<u>Hendrix v. Page,</u> 986 F.2d 195 (7 th Cir. 1993)(Posner, J.)	21
<u>Hispanic Society of NYC v. NYC Police Department,</u> 806 F.2d 1147 (2 nd Cir. 1986)	19
<u>Junger v. Daley,</u> 209 F.3d 481 (6 th Cir. 2000)	21, 46
<u>Kaplan v. Rand,</u> 192 F.3d 60 (2 nd Cir. 1999)	19
<u>Keith v. Volpe,</u> 118 F.3d 1386 (9 th Cir. 1997)	16, 18, 20
<u>Kenny v. Quigg,</u> 820 F.2d 665 (4 th Cir. 1987)	17
<u>Liberty Mutual Ins. Co. v. Commercial Union Ins. Co.,</u> 978 F.2d 750 (1 st Cir. 1992)	15
<u>Los Angeles News Service v. Conus Communications Co.,</u> 969 F. Supp. 579 © D Cal. 1997)	36, 37
<u>Los Angeles News Service v. Reuters Television International,</u> 149 F.3d 987 (9 th Cir. 1998)	35
<u>Mainstream Loudoun v. Board of Trustees,</u> 2 F. Supp. 2d 783 (E.D. Va. 1998); 24 F. Supp. 2d 552 (1998)	9, 10, 29
<u>Marino v. Ortiz,</u> 484 U.S. 301 (1988)	19, 20
<u>Metze v. May Department Stores,</u> 878 F. Supp. 756 (WD Pa. 1995)	36, 37
<u>National Football League v. Primetime 24 Joint Venture,</u> 2000 U.S. App. LEXIS 8275 (2 ^d Cir. 2000)	37

<u>National Football League v. TVRadio Now Corp,</u> __F.3d __, 53 U.S.P.Q. 2d 1831 (WD Pa 2000)	36, 37
<u>National Wildlife Federation v. Gorsuch,</u> 744 F.2d 963 (3 rd Cir. 1984)	33
<u>NBA Properties v. Gold,</u> 895 F.2d 30 (1 st Cir. 1990)	24
<u>Nelson v. Adams,</u> __U.S. __, 120 S.Ct. 1579 (2000)	23
<u>New York State Club Ass’n, Inc., v. City of New York,</u> 487 U.S. 1 (1988)	18
<u>Pennoyer v. Neff,</u> 95 U.S. 714 (1878)	23
<u>ProCD v. Zeidenberg,</u> 86 F.3d 1447 (7 th Cir. 1996)	49
<u>Project BASIC v. Kemp,</u> 947 F.2d 11 (1 st Cir. 1991)	23
<u>In re Providence Journal,</u> 820 F.2d 1342, 1353 (1 st Cir. 1986) <u>mod. en banc on other gr.</u> 820 F.2d 1359 (1 st Cir. 1987)	25
<u>Regal Knitwear Co. v. NLRB,</u> 324 U.S. 9 (1945)	20
<u>Reno v. ACLU,</u> 521 U.S. 844 (1997)	9, 22, 29
<u>S.E.C. v. Wencke,</u> 783 F.2d 829(9 th Cir. 1986)	17
<u>Sega Enter. Ltd. v. Accolade, Inc.,</u> 977 F.2d 1510 (9 th Cir. 1992)	41, 42-43, 46
<u>Sierra Fria Corp. v. Donald J. Evans,</u> 127 F.3d 175 (1 st Cir. 1997)	15
<u>Sony Computer Entertainment, Inc. v. Connectix Corp.,</u> 203 F.3d 596 (9 th Cir. 2000)	3, 4, 40, 41, 42, 43, 46, 47, 48
<u>Sony Corp. v. Universal City Studios, Inc.,</u> 464 U.S. 417 (1984)	46
<u>Speiser v. Randall,</u> 357 U.S. 513 (1958)	24

<u>Subafilms, Ltd. v. MGM-Pathe Communications Co.,</u> 24 F.3d 1088 (9 th Cir. 1994) (en banc)	35
<u>Twin Books Corp v. Walt Disney Co.,</u> 83 F.3d 1162 (9 th Cir. 1996)	35
<u>United Dictionary v. G&C Merriam Co.,</u> 208 U.S. 260 (1908)	35
<u>United States Catholic Conference v. Abortion Rights Mobilization, Inc.,</u> 487 U.S. 72, 77 (1988)	39
<u>United States v. Valle,</u> 72 F.3d 210 (1 st Cir. 1995)	15
<u>United States v. Zapata,</u> 18 F.3d 971 (1 st Cir. 1994)	15
<u>Update Art v. Modiin Publications,</u> 843 F.2d 67 (2d Cir. 1988)	35, 39
<u>U.S. v International Brotherhood of Teamsters,</u> 931 F.2d 177 (2 nd Cir. 1991)	17
<u>Vault v. Quaid,</u> 847 F.2d 255 (5 th Cir. 1988)	49, 50
<u>Virginia v. American Booksellers,</u> 484 U.S. 383 (1988)	21, 22
<u>Williams v. Morgan,</u> 111 U.S. 684 (1884)	17
<u>Zenith Radio Corporation v. Hazeltine Research,</u> 395 U.S. 100 (1969)	16, 23
STATUTES AND RULES	
17 U.S.C. §101	1
17 U.S.C. §106(4)	37, 38
17 U.S.C. §106(5)	37
17 U.S.C. §107	39-40, 44
28 U.S.C. §1291	2
28 U.S.C. §1331	1
28 U.S.C. §1332	1

28 U.S.C. §1338	1, 34, 38
47 U.S.C. §230(d)	9
Fed. R. Civ. Pro. 12(h)	18
Fed. R. Civ. Pro. 65(d)	14, 32, 34
S. 97, 106 th Cong., 1 st Sess. (1999)	9
S. 1545, 106 th Cong., 1 st Sess. (1999)	9
H.R. 368, 106 th Cong., 1 st Sess. (1999)	9
OTHER AUTHORITIES	
Keith Bradsher, “Town Rejects Bid to Curb Library's Internet Access,” <u>N.Y. Times</u> , Feb 27, 2000	9, 10
Hiawatha Bray, “Hard Core Fixes to On-line Porn,” <u>Boston Globe</u> , Oct. 15, 1996	9
Hiawatha Bray, “A Faulty Censor,” <u>Boston Globe</u> , Dec. 30, 1999	9
Tom Callahan, <u>N.Y. Times</u> , May 14, 2000, 14WC, at 9	10
Matt Carroll, “Cyber Patrol v. Christian Right,” <u>Boston Globe</u> , June 21, 1998	9
Paul Goldstein, <u>Copyright: Principles, Law and Practice</u> § 16.0 at 675 (1989)	35
Amy Harmon, “Ideological Foes Meet on Web Decency,” <u>N.Y. Times</u> , Dec. 1, 1997	10
Jansson and Skala, “The Breaking of Cyber Patrol.”	4
Carrie Kirby, “A World of Safe Havens in the Chaos of Cyberspace,” <u>San Francisco Chronicle</u> , June 1, 2000	9-10
M. Lemley, Intellectual Property and Shrink Wrap Licenses, 68 <u>S. Cal. L. Rev.</u> 1239 (1995)	50
“Library Net filter proposal defeated,” <u>USAToday</u> , Feb. 23, 2000	9
Joshua Quittner, “Web Censorware,” <u>Time</u> , July 13, 1998	10
David Roeder, “Filtering Software Not Always Effective,” <u>Chi. Sun-Times</u> , Feb. 27, 2000	10
Seth Schiesel, “How Web Smut is Regulated May Depend on Tools to Filter It,” <u>N.Y. Times</u> , Mar. 24, 1997	10

Irwin B. Schwartz, “Keep Copyrights Safe on the Net,” <u>Boston Globe</u> , May 16, 2000	16
Jonathan Weinberg, “Hardware-Based ID, Rights Management, and Trusted Systems,” 52 <u>Stanford L. Rev.</u> 1251, 1252, n.2 (forthcoming 2000)	4
Jonathan Weinberg, “Rating the Net,” 19 <u>Comm/Ent</u> 453, 459-470 (1997)	30
Wright, Miller & Kane, <u>Federal Practice and Procedure</u> , 11A at 343	21
http://www.cyberpatrol.com	3
http://www.islandnet.com/~mskala/cpbfaq.html	27, 28, 30
www.aclu.org/courts/loudoun_brief	30
www.censorware.org	30
www.microsys.com/news/Press/000328	16
www.peacefire.org	30

REASONS WHY ORAL ARGUMENT SHOULD BE HEARD

The district court said this case raised a “complex and significant legal issue relating to copyright law.” It also said that the case “raises a most profound societal issue” concerning the use of computer software that blocks users from accessing Internet sites deemed “objectionable.” The district court, based on the unsupported affidavits of the plaintiffs and an unprecedented and unwarranted expansion of U.S. copyright law, came down squarely on one side of that profound societal issue (endorsing plaintiffs’ product). It enjoined speech by the product’s critics that illustrated flaws in the product. Then, it extended the injunction not only to defendants, but to unrelated individuals all over the world, expressly denying them the opportunity to present evidence that would contradict plaintiffs. Because of the importance of this order, which silences speech on a matter of public concern, and because review may involve some unfamiliar technical concepts, oral argument will facilitate the Court's understanding of the issues.

JURISDICTIONAL STATEMENT

Plaintiff Microsystems asserted jurisdiction pursuant to 28 U.S.C. §§1331 and 1332, alleging violations of the Copyright Act, 17 U.S.C. §101 *et. seq.* The district court found that it had jurisdiction pursuant to 28 U.S.C. §1338.

However, the district court did not have subject matter jurisdiction over this case (or personal jurisdiction over appellants). The acts alleged in the Complaint, even if accepted, took place entirely out of the country and the Copyright Act does not have extraterritorial effect. See Argument, Section IV.

This Court has jurisdiction pursuant to 28 U.S.C. §1291 because this is an appeal from a final order of the district court disposing of all parties' claims. The district court's order was issued on March 28, 2000. Notice of Appeal was timely filed on April 4, 2000.

ISSUES PRESENTED

1. When appellants appeared in the district court to oppose entry of an order, when plaintiffs assert that appellants are bound by the order, when appellants were served with the order in order to bind them to it, and when the order has had the effect of suppressing their speech, do appellants have standing to challenge the order?

2. Did the district court violate due process by refusing to tell appellants whether the order prohibited their speech or not and by refusing appellants the opportunity to challenge the validity of the order?

3. Did the district court have subject matter jurisdiction in a copyright case when the only copying alleged to have been done was done out of the country?

4. Even if subject matter jurisdiction existed, was any copying done by

defendants legal as a “fair use” where that copying was a necessary prerequisite to public comment on a “most profound societal issue?”

STATEMENT OF THE CASE AND STATEMENT OF FACTS

This case was filed on March 15, 2000, on behalf of plaintiffs, the corporate owners of a product called Cyber Patrol (hereinafter Cyber Patrol). Addendum [Add.] p. 1, 3, ¶¶1-3, 12. Defendants Jansson and Skala (Jansson/Skala) are residents of Sweden and Canada. Appendix [App.] p. 9, ¶¶3-4. The Complaint alleged that Jansson/Skala violated Cyber Patrol’s copyright rights when they “reverse engineered” Cyber Patrol.¹ App. p. 12, ¶21.

Cyber Patrol is a product used by individuals, schools, libraries, corporations and others. App. p. 8, ¶1; <http://www.cyberpatrol.com>. When installed on a computer, it prevents the person using that computer from having access to Internet web sites that are placed on a list created by Cyber Patrol and that are deemed “objectionable” according to a variety of criteria. *Id.*; Add. p. 1, ¶3. The list of blocked sites is kept secret by Cyber Patrol. Jonathan Weinberg, “Hardware-Based ID, Rights Management, and Trusted Systems,” 52 Stanford L.

¹ Reverse engineering" refers to the use of one or more methods of gaining access to the functional elements of a software program, such as observing the program in operation, examining the instructions underlying the software, or using a program known as a "disassembler" to translate the binary machine-readable "object code" that runs on the computer into the human-readable words and symbols known as "source code." See generally Sony Computer Entertainment v. Connectix Corp., 203 F.3d 596, 599-600 (9th Cir. 2000).

Rev. 1251, 1252, n.2 (forthcoming 2000). As the district court noted, the use of such products is controversial and raises “most profound” issues, particularly since such products often block as objectionable such harmless sites as the map of Disney World.

Cyber Patrol alleged that Jansson/Skala reverse engineered Cyber Patrol and then, based on their knowledge of the manner in which Cyber Patrol worked, wrote their own computer code. App. pp. 10-11, ¶14. This newly written code, not itself copyrighted by Cyber Patrol and not alleged to contain any of Cyber Patrol’s program or code, made it possible to view the list of sites that the product censors. App. p. 33. It was possible to view the list only if you already lawfully possessed a copy of Cyber Patrol. App. p. 33. Jansson/Skala placed their computer code on their own web sites hosted by Internet Service Providers in Sweden and Canada. App. p. 9, ¶¶ 5-6. Jansson/Skala gave permission for others to copy the code. Jansson and Skala, “The Breaking of Cyber Patrol.”

The Complaint does not allege that the reverse engineering, and therefore the alleged copyright violation, occurred in the United States. It implies that it occurred in Canada and/or Sweden. App. p. 9-12.

Appellants Jaquith et. al are individuals who run “mirror” sites. App. p. 19, ¶6; p. 62, ¶2; pp. 86-87, 91, 93. Appellants placed copies of the code written by Jansson/Skala on their web sites (or “mirror”-ed it). Id.; App. pp. 39-40.

On March 17, 2000, Cyber Patrol sought a temporary restraining order

against Jansson/Skala “and those in active concert or participation with them” prohibiting posting of the Jansson/Skala code on the Internet. App. pp. 41-43. Cyber Patrol asserted that one of the reasons it needed a TRO was to bind mirror sites such as those run by the appellants. App. p. 19, ¶6. The operators of the mirror sites, such as appellants, were not made defendants. The district court granted the TRO on an ex parte basis on March 17. App. pp. 41-43. The court set March 27, 2000, for a hearing on a preliminary injunction. Id.

Cyber Patrol had already presented evidence to the district court that at least one of the appellants was not “in active concert” with Jansson/Skala. According to Cyber Patrol, defendant Skala expressly said that at least one of appellants was not involved in their actions. App. p. 33 (“Peacefire [run by appellant Haselton] deserves credit and blame for many things, but not for this particular project. We did this independently of them. It wasn’t a Peacefire project.”)(emphasis added).

Nevertheless, Cyber Patrol served the TRO on appellants by email along with a cover letter suggesting that appellants were “in active concert” and were therefore bound by the order. App. p. 63, ¶4; pp. 86-88, 91, 93-94; Add. p. 5, ¶¶20-21. Cyber Patrol also suggested they “retain counsel in Massachusetts.” App. p. 88. Cyber Patrol also served subpoenas on appellants seeking information. App. pp 58, ¶4; 86, 91, 93.

Counsel for appellants filed an appearance and a motion to permit one of

counsel to appear pro hac vice. App. pp. 44-48. Appellants also filed a Motion to Quash the subpoenas. App. p. 49. Appellants also filed an Opposition to Motion for Preliminary Injunction. App. p. 3, docket entry 9. Appellants appeared before the district court on March 27, 2000, to argue that no injunction should issue or, at least, the injunction should not bind mirror site operators such as appellants. App. p. 3-4, docket entries 9, 11. The court granted the motion for counsel to appear pro hac vice on behalf of appellants and permitted appellants to present argument in opposition to the entry of an injunction that would bind them. App. p. 56; p. 4, docket entry 11.

At the start of the March 27 hearing (on Cyber Patrol's motion for a preliminary injunction), Cyber Patrol advised the court that it had settled with Jansson/Skala who agreed to "never again seek to publish software designed to defeat Cyber Patrol." App. p. 59, ¶6; Add. p. 6, ¶26. Cyber Patrol proffered a proposed Final Injunction which bound Jansson/Skala and those "in active concert" from posting the code that Jansson/Skala had written, and which authorized service of the order on "all persons posting [the code] on the Internet." App. pp. 57-61. In an affidavit by counsel, Cyber Patrol asserted that all individuals who ran mirror sites, such as appellants, were "in privity" with Jansson/Skala "because they copied the content directly from Jansson's web page or from someone else who did so." App. p. 62, ¶3. Cyber Patrol asserted that all such web sites could be bound by the injunction. App. p. 62, ¶¶3, 5.

Appellants asked the court to refuse to enter the final injunction for a variety of legal reasons discussed below. Among the arguments explicitly made by appellants was that the court did not have personal jurisdiction over them and that the court did not have subject matter jurisdiction to enter the order. App. p. 52, n.3; p. 3, docket entry 9, Opposition to Motion for Preliminary Injunction. Appellants expressly denied the facts as presented by Cyber Patrol. Opposition to Motion for Preliminary Injunction at 5. Appellants also asked the court, if it decided to enter the final injunction, to clarify whether appellants were bound by it. *Id.* at 1. The following day, appellants asked the court for permission to file a supplemental memorandum of law opposing the final injunction. App. p. 83. The court granted that request. App. p. 85.

The court entered a final injunction one day later on March 28, 2000. The injunction binds Jansson/Skala “and all persons in active concert or participation” with them. Add. p. 16. The injunction requires Cyber Patrol serve it on “all persons in active concert or participation” by “certified mail to last known address.” Add. p. 17. Cyber Patrol has served two of appellants with a copy of the injunction as well as many other mirror site operators all over the world. App. pp. 86-88; App. p. 91, ¶5; App. p. 94, ¶5. Cyber Patrol asserted in a press release that all mirror sites, like appellants, are bound by the injunction.

The court found, without any evidence having been taken and based on the conclusory affidavit of Cyber Patrol’s counsel, that “many” of the persons who

created the mirror sites did so for the “avowed purpose of seeking to prevent this Court from awarding meaningful relief.” App. p. 63, ¶3; Add. p. 4, ¶15. The court made no findings specifically with respect to appellants.

Finally, the court held that “[a]ny violation of this injunction shall be determined by the Court only on the filing by Plaintiffs of a Motion for an Order to Show Cause Why a Certain Person or Entity Should Not Be Held in Contempt and after full hearing thereon.” Add. p. 17 (emphasis added). The court also granted appellants’ motion to quash the subpoenas. App. p. 82.

Appellants were engaged in valuable speech on a matter of national importance. The value of products such as Cyber Patrol has been a matter of enormous public debate over the last few 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 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 27, 2000, at A12.) Legislation has been introduced in Congress and in the states requiring the use of such products in libraries and schools. S.

97, 106th Cong., 1st Sess. (1999); S. 1545, 106th Cong. 1st Sess. (1999); H.R. 368, 106th Cong., 1st Sess. (1999). Federal law already requires that all Internet Service Providers give subscribers information about the availability of such software. 47 U.S.C. §230(d).

There have been numerous articles in the press about products such as Cyber Patrol. See e.g. Matt Carroll, “Cyber Patrol v. Christian Right,” Boston Globe, June 21, 1998, at 2; Hiawatha Bray, “A Faulty Censor,” Boston Globe, Dec. 30, 1999, at D1; Hiawatha Bray, “Hard Core Fixes to On-line Porn,” Boston Globe, Oct. 15, 1996, at C1; Carrie Kirby, “A World of Safe Havens in the Chaos of Cyberspace,” San

Francisco Chronicle, June 1, 2000; Tom Callahan, N.Y. Times, May 14, 2000, 14WC, at 9; Keith Bradsher, “Town Rejects Bid to Curb Library’s Internet Access,” N.Y. Times, Feb. 27, 2000, at A12; Joshua Quittner, “Web Censorware,” Time, July 13, 1998, at 84; Amy Harmon, “Ideological Foes Meet on Web Decency,” N.Y. Times, Dec. 1, 1997, at D1; David Roeder, “Filtering Software Not Always Effective,” Chi. Sun-Times, Feb. 27, 2000, at 2; Seth Schiesel, “How Web Smut is Regulated May Depend on Tools to Filter It,” N.Y. Times, Mar. 24, 1997, at D5. A NEXIS search for “filtering software” for just four major papers shows over 1000 stories. A similar NEXIS search for Cyber Patrol itself shows 250 stories prior to January 1, 2000.

Many press accounts of products such as Cyber Patrol 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 (which was a plaintiff in the case). It also blocked a map of Disney World.

The Jansson/Skala code, mirrored by appellants, allows lawful owners of the product to view the blocked sites list. In so doing, it contributes important information to this public debate. Moreover, neither Jansson/Skala nor appellants obtained any financial advantage or remuneration for their speech.

The district court acknowledged this debate, and its importance. It said that this case raised a “most profound societal issue.” Add. p. 17. Then, based solely on the unsupported affidavits of Cyber Patrol’s counsel and in the face of appellants’ assertion that the facts presented by Cyber Patrol were erroneous, the district court found that Jansson/Skala (and presumably appellants) had acted in a manner “inconsistent with the general public good,” Add. p. 12, ¶48, and that the balance of hardships favored Cyber Patrol. Add. p. 13, ¶51. The court then, in effect, endorsed the value of Cyber Patrol, Add. p. 18, and suppressed the criticism of it because it would “adversely affect the potential market.” Add. p.

12, ¶50.

Appellants sought a stay from the district court. App. p. 5, docket entry 25. That application was denied. The district court said that it “refused to issue an advisory ruling for the benefit of nonparties” and relegated them to “the usual procedure for adjudication of any contempt.” App. p. 96-97. The court also held that appellants “have no standing to pursue any appeal.” Id. Appellants sought a stay, or in the alternative, expedited appeal, from this Court. The stay was denied on May 22, 2000, and the appeal was expedited. Order, May 22, 2000. The Court further said that “[w]e defer resolving the issue of standing to appeal asserted by nonparties Jaquith, Haisley, and Haselton until after full briefing and argument.” Id.

As a result of the district court’s orders, the appellants removed the speech from their mirror sites. App. p. 86, ¶2; p. 91, ¶3; p. 93, ¶3; see also Add. p. 5, ¶22. The effect of the court’s order is to leave appellants chilled from engaging in speech by the very real prospect of a contempt finding if they resume the speech and the district court, on Cyber Patrol’s motion, deems them to have been bound by the order -- a state of uncertainty that, as argued below, is constitutionally unacceptable. Appellants can presumably argue that they are not “in active concert,” but that argument is available only if appellants risk contempt, at which point they may well not be able to challenge the merits of the underlying decree. This result -- that speech can be enjoined without the speaker

ever having the chance to be heard on the factual and legal findings underlying such an injunction -- is untenable under basic principles of law.

SUMMARY OF ARGUMENT

Appellants are engaged in speech that was not copyrighted by Cyber Patrol and concerns a matter of enormous public debate. Nevertheless, by filing a copyright action and settling with the defendants Jansson/Skala, Cyber Patrol has obtained a judgment the effect of which is to prevent appellants from engaging in that speech. Cyber Patrol served appellants with the order and repeatedly asserted in court and in public fora that appellants are bound by the order. Simultaneously, Cyber Patrol has vigorously sought to prevent appellants from obtaining a determination of the applicability of the injunction to them or a determination of validity of the order. Appellants' position in this Court is a simple one. Before their speech can be enjoined, they are entitled to raise any defenses and have a hearing on the validity of the injunction, particularly where, as here, the court did not have subject matter jurisdiction to enter the injunction.

First, even though appellants were not parties in the district court (because they did not wish to waive a defense of personal jurisdiction), they have standing to appeal. They appeared in the district court, filed motions (which were ruled upon) and argued. Moreover, Cyber Patrol has served them with the order and asserted they are bound by it. Section II., infra.

Second, appellants sought to obtain from the district court a determination

of whether they were bound by the order or not. The district court's refusal to provide that determination, particularly where the effect is to chill constitutionally protected speech, violated due process. Section III.A., infra.

In addition, where a person seeks on a timely basis to be heard on the validity of an order which purports to bind them, that party is entitled as a matter of due process to a hearing on the validity of the order. The district court denied appellants that hearing. It held that their only remedy was to subject themselves to a future contempt motion at which they would not be permitted to contest the validity of the order and at which they must risk imprisonment or fine. The district court's reliance on Fed. R. Civ. Pro. 65 for this procedure was error and the procedure violated due process. Section III.B, infra.

Third, the district court did not have subject matter jurisdiction to issue the order. The only allegation was that a copyright violation took place in either Sweden or Canada. Because the U.S. copyright law does not have extraterritorial effect, the court was without jurisdiction. Section IV, infra.

Finally, even if the court had subject matter jurisdiction, Jansson/Skala's use of Cyber Patrol was protected by the "fair use" doctrine. The district court refused to determine the applicability of the "fair use" doctrine when Jansson/Skala settled. However, to the extent the injunction binds appellants, appellants are entitled to show that it was unjustified because Jansson/Skala acted legally. Appellants, if permitted, could present facts to show that Jansson/Skala's

use of Cyber Patrol was a “fair use” and was otherwise legal. Section V, infra.

ARGUMENT

I. THE COURT SHOULD REVIEW THE ISSUES IN THIS CASE DE NOVO.

All of the issues raised on this appeal are legal issues and subject to de novo review by this Court. E.g. Sierra Fria Corp. v. Donald J. Evans, 127 F.3d 175, 181 (1st Cir. 1997); Liberty Mutual Ins. Co. v. Commercial Union Ins. Co., 978 F.2d 750, 757 (1st Cir. 1992). See also United States v. Valle, 72 F.3d 210, 214 (1st Cir. 1995); United States v. Zapata, 18 F.3d 971, 975 (1st Cir. 1994).

II. APPELLANTS HAVE STANDING TO APPEAL.

Although appellants were not formally parties to the proceeding below, they do have standing to appeal. Appellants filed a notice of appearance in the district court and presented oral argument against the entry of the injunction. The district court granted three motions filed by appellants (to argue pro hac vice, to quash the subpoenas, to submit a supplemental brief) and denied two (for a stay, to file supplemental affidavits). Of the five motions, the court denied only the last one on the basis that appellants lacked standing, the motion for a stay. App. p. 97. All others were decided on the merits. App. pp. 56, 82, 85, 95.

Cyber Patrol has repeatedly asserted that appellants are bound by the orders in this case. Cyber Patrol asserted that it needed a a TRO in large part because it sought to bind mirror site operators such as appellants. App. p. 19, ¶6. Cyber Patrol submitted an affidavit asserting that mirror sites were in privity with Jansson/Skala and would, therefore, be bound by the order. App. p. 62, ¶3. Cyber Patrol’s own press release about the injunction said that: “[t]he Court order ... also applies to so called ‘mirror’ sites...” www.microsys.com/news/Press/000328; See also Irwin B. Schwartz, “Keep Copyrights Safe on the Net,” Boston Globe, May 16, 2000 at F4 (bragging that the order applied to mirror sites). Finally, as required by the district court’s order, Cyber Patrol served the order on appellants in order to bind them and suggested they needed to retain Massachusetts counsel. Add. p. 17; App. pp. 86-92.

Nonparties may appeal an order where “a lower court specifically directs an order at a nonparty or enjoins it from a course of conduct.” Dopp v. HTP Corp., 947 F.2d 506, 512 (1st Cir. 1991) (citing Zenith Radio Corp. v. Hazeltine Research, Inc., 395 U.S. 100, 108-12 (1969)). As discussed, Cyber Patrol asserts that appellants are bound and thus, under Dopp, appellants have a right to appeal.

More specifically, the general rule precluding appeals by nonparties does not apply to nonparties (1) that have participated in the proceedings below, and (2) when the equities weigh in favor of hearing the appeal. Keith v. Volpe, 118

F.3d 1386, 1391 (9th Cir. 1997) (holding that nonparty had standing to appeal although he did not seek to intervene because he filed a Memorandum of Points and Authorities, participated in oral argument, and because plaintiffs sought to have preliminary injunction applied to him while also attempting to “thwart[] the nonparty’s right to appeal”) (citing S.E.C. v. Wencke, 783 F.2d 829, 834 (9th Cir. 1986)); Caplan v. Braverman & Kaskey, 68 F.3d 828, 836 (3rd Cir. 1995) (holding that nonparty had standing to appeal although it did not seek to intervene because it participated in hearing on defendants’ emergency motion, it must uphold its contractual terms with its policy holders, and it has a stake in the outcome of pending settlement negotiations) (citing Binker v. Pennsylvania, 977 F.2d 738, 745 (3rd Cir. 1992)); Curtis v. City of Des Moines, 995 F.2d 125, 128 (8th Cir. 1993) (holding that nonparties had standing to appeal although they did not seek to intervene because they actively participated in post-trial executions on the judgment, they contested issues later raised on appeal, they had an interest which was affected by the lower court’s judgment, and because the district court treated them as parties by accepting their briefs); Kenny v. Quigg, 820 F.2d 665, 668 (4th Cir. 1987) (holding that nonparty had standing to appeal because he participated significantly in the district court proceedings by being kept apprised of the fiduciary’s activities and of the proceedings in the district court, his memorandum and argument were considered by the court, and he had a substantial interest in the outcome of the district court proceedings); U.S. v

International Brotherhood of Teamsters, 931 F.2d 177, 183 (2nd Cir. 1991). See also Williams v. Morgan, 111 U.S. 684 (1884) and cases cited therein (nonparties may appeal in appropriate cases).

Appellants did participate in the proceedings below. The equities favor allowing appellants to appeal. When a nonparty has been forced into the proceeding against his will, and attempts are subsequently made to “thwart the nonparty’s right to appeal by arguing that he lacks standing,” the equities weigh in favor of conferring standing on the nonparty. Keith, 118 F.3d at 1391. Ultimately, the balancing of the equities favors allowing the appellants’ appeal to proceed because the injunction has a direct effect on them. See, e.g., Caplan, 68 F.3d at 836; Curtis, 995 F.2d at 128, Dopp, 947 F.2d at 512. Moreover, this injunction restricts speech and standing rules have often been viewed in a more relaxed fashion in free speech cases. New York State Club Ass’n, Inc., v. City of New York, 487 U.S. 1, 14-15 (1988) (quoting City Council v. Taxpayers for Vincent, 466 U.S. 789, 798 (1984)).

The equities also favor appellants for another reason. If appellants had filed a motion to intervene, they would have had to concede that the court had personal jurisdiction over them, a proposition which they explicitly denied. Fed. R. Civ. Pro. 12(h); Opposition to Motion for Preliminary Injunction at 1, n.1; App. 52, n. 3.

If appellants are not permitted to appeal, they may never have the

opportunity to contest the facts or the conclusions of law that form the basis for the injunction. Those facts were found by the district court solely on the basis of the Complaint and an affidavit by counsel for Cyber Patrol. The district court has held that appellants may never be heard, except in the context of contempt. Add. p. 17. “Ordinarily the validity and terms of an injunction are not reviewable in contempt proceedings.” G. & C. Merriam Co. v. Webster Dictionary Co., 639 F.2d 29, 34 (1st Cir. 1980). Thus, to deny appellants standing is to deny them their due process right to be heard. See section III, infra.

The district court found that appellants did not have standing relying on Marino v. Ortiz, 484 U.S. 301 (1988) which affirmed Hispanic Society of NYC v. NYC Police Department, 806 F.2d 1147 (2nd Cir. 1986). In the context of whites objecting to a race-conscious settlement, Marino held that where a “nonparty has an interest that is affected by the trial court’s judgment,” the “better practice” is for that nonparty to intervene. Marino, 484 U.S. at 304. Cyber Patrol argues that Hispanic Society and Marino stand for the proposition that a person who does not intervene may not appeal. However, the Second Circuit has directly rejected Cyber Patrol’s interpretation. In Kaplan v. Rand, 192 F.3d 60, 68 (2nd Cir. 1999), the court said that the Supreme Court in Marino had “not reject[ed] our rule permitting appeal by nonparties with affected interests ...[T]he later affirmance of Felzen v. Andreas, 134 F.3d 873 (7th Cir. 1998) aff’d sub nom California Pub. Employees v. Felzen, 525 U.S. 315

(1999)(per curiam)] demonstrates that the Court has yet to reject a rule that allows an appeal by a nonparty having an interest affected by the judgment of the trial court.”

Moreover, even if this Circuit is unpersuaded by the Second Circuit’s standard, appellants have much more than “an interest that is affected.” Either appellants are bound by the order, in which case they have been haled into court, or they are not, in which case the court should free them from the risk of contempt. As the Keith court specifically held, Marino is inapplicable when, as here, the appellant has been “haled” into court over his objections. 118 F.3d at 1391, n. 7; Curtis, 995 F.2d at 128. This Court in Dopp and the five other Circuits cited above correctly agree that in cases such as this, a nonparty has standing to appeal.

III. THE DISTRICT COURT’S REFUSAL TO DETERMINE THE APPLICABILITY OF ITS ORDER TO APPELLANTS AND ITS CONCLUSION THAT APPELLANTS, EVEN IF FOUND TO BE BOUND BY THE ORDER, MAY NOT CHALLENGE ITS LEGALITY, VIOLATED DUE PROCESS.

A. The District Court Erred in Refusing To Tell Appellants If The Order Applied to Them or Not.

Due process requires that appellants be able to determine, without risking contempt, if the order applies to them. In Regal Knitwear Co. v. NLRB, 324 U.S. 9, 15 (1944), the Supreme Court said that “[W]e think courts would not be apt to withhold a clarification in the light of a concrete situation that left parties or ‘successors and assigns’ in the dark as to their duty toward the court...

[O]rders are [not] issued ... for the entrapment of parties, and courts no less than parties desire to avoid unwitting contempts as well as to punish deliberate ones.” See also Wright, Miller & Kane, Federal Practice and Procedure, 11A at 343 (“when an interested individual is confused as to the applicability of an order to him ..., he may request the granting court to construe or modify the decree.”) This due process principle underlies many legal doctrines. Thus, for example, a person need not risk arrest in order to challenge the constitutionality of a criminal statute that prohibits speech. Virginia v. American Booksellers Ass’n, 484 U.S. 383, 392-93 (1988).

Appellants followed this principle and asked the district court to determine if the order applied to them or not. App. p. 4, docket item 11. The district court refused to answer that question, holding that to do so would be to issue an advisory opinion. App. p. 96 . The Seventh Circuit has explicitly rejected that rationale. “[A] person subject to an injunction always has the right to ask the court that is administering it whether it applies to conduct in which the person proposes to engage. If this looks like a request for an ‘advisory opinion,’ it is one that even a federal court can grant in order to prevent unwitting contempts.” Hendrix v. Page, 986 F.2d 195, 200 (7th Cir. 1993)(Posner, J.).

This principle is of particular importance in this case. Appellants are engaged in speech. Junger v. Daley, 209 F.3d 481 (6th Cir. 2000)(computer code is speech). The injunction prohibits speech. If appellants are unwilling to risk

contempt, including fine and imprisonment, they must refrain from that speech. The vagueness of the applicability of the order to them means that they will never know whether the injunction applies to them or not. The Supreme Court has recently reaffirmed the dangers of vague restrictions on speech in the context of the Internet. In Reno v. ACLU, 521 U.S. 844, 872 (1997), the Court said that “vagueness ... raises special First Amendment concerns because of its obvious chilling effect on free speech.” Vagueness, the Court said “unquestionably silences some speakers whose messages would be entitled to constitutional protection.” Id. at 874; Grayned v. City of Rockford, 408 U.S. 104, 109 (1972). This vagueness is further aggravated, the Court said when the potential penalties for violation include imprisonment. “[T]he severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images.” Reno, 521 U.S. at 872. If this order were a statute, appellants would unquestionably have standing to challenge it. American Booksellers, 484 U.S. at 392-93. By successfully persuading the district court to leave the applicability of the order to appellants vague and requiring appellants to risk imprisonment in order to test its applicability, Cyber Patrol will have accomplished precisely the kind of chill of speech caused by vague laws that the First Amendment prohibits, through a procedure that violated the due process clause.

B. The District Court Erred in Holding That Persons Who May Be Bound By An Order and Who Promptly Seek to Contest The Validity of That Order

May Not Ever Do So.

Even if the district court had told appellants that they were bound by the order, the process it adopted still would have violated the due process clause. It is an “elementary” rule of civil procedure and due process that a court cannot enter a judgment against someone who “has not been made a party by service of process.” Zenith Radio Corporation v. Hazeltine Research, 395 U.S. 100, 110 (1969); Hansberry v. Lee, 311 U.S. 32, 40-41 (1940); Pennoyer v. Neff, 95 U.S. 714 (1878)); Chase National Bank v. City of Norwalk, 291 U.S. 431, 438 (1934); Project BASIC v. Kemp, 947 F.2d 11, 19 (1st Cir. 1991) (“... non-parties are generally not bound by court orders because they have not had their day in court; in other words they have not had their opportunity to challenge the order’s validity,” citing G. & C. Merriam v. Webster, 639 F.2d 29 (1st Cir. 1980)) See Alemite Manufacturing v. Staff, 42 F.2d 832, 833 (2nd Cir. 1930)(Learned Hand) (“[N]o court can make a decree which will bind any one but a party.”). The Supreme Court has just reaffirmed the fundamental nature of this element of due process, unanimously, and held that even where there is a close identity between the party and the nonparty, the nonparty still is entitled to due process. Nelson v. Adams, ___ U.S. ___, 120 S.Ct. 1579 (2000).

As in the prior section, these concerns are also heightened because this arises in the context of speech. The First Amendment has a due process component. Speiser v. Randall, 357 U.S. 513, 521 (1958) (“When the state

undertakes to restrain unlawful advocacy it must provide procedures [to determine the facts of the case] which are adequate to safeguard against infringement of constitutionally protected rights--rights which we value most highly and which are essential to the workings of a free society.") Freedman v. Maryland, 380 U.S. 51, 58 (1965); Fantasy Book Shop, Inc. v. City of Boston, 652 F.2d 1115 (1st Cir. 1981).

Even though appellants sought on a timely basis to raise defenses to the validity of the order, the district court believed these fundamental due process considerations to be irrelevant. The court held that the appellants would have the opportunity to exercise their due process rights only in a subsequent contempt proceeding. Add. p. 17.

Under the procedures outlined by the court, appellants may never have the opportunity to contest the facts or the legal conclusions on which the injunction is based. See NBA Properties v. Gold, 895 F.2d 30, 34 (1st Cir. 1990) ("a court may ordinarily impose [contempt] without providing the party an opportunity to challenge the validity of the decree itself..."); G & C. Merriam v. Webster, 639 F.2d 29 (1st Cir. 1980).² In this case, the court's findings were based solely on the affidavits of one party's counsel (and the Verified Complaint). The court's

² A person may challenge the facial invalidity of an order under the First Amendment even in the context of contempt. In re Providence Journal, 820 F.2d 1342, 1353 (1st Cir. 1986) mod. en banc on other gr. 820 F.2d 1359 (1st Cir. 1987). However, this puts a far heavier burden on the objecting person than if they had been heard initially. Moreover, many other defenses cannot be asserted.

findings included such broad generalities as “inconsistent with the general public good” and in the “public interest” and “irreparable harm” to the “public.” Add. pp. 1-6. The court justified its order with an opinion that amounts to a strong endorsement of Cyber Patrol and a suggestion that the Jansson/Skala code would allow “noxious and insidious ideas” to corrupt children. Add. p. 18. Particularly under these circumstances, appellants, who are at least chilled from speaking by the order, were entitled as a matter of due process to be heard on the validity of the those findings and opinions.

There are a number of facts that the appellants could have presented if permitted that would have contradicted the court’s findings. Those facts would have illustrated that this “most profound” dispute was far more complicated than the district court understood and should not have been resolved by a procedure in which only one side presented evidence.³

The district court found that an injunction was necessary because the “public will continue to suffer irreparable harm” and that the “infringer” (Jansson/Skala) would suffer no harm because it consented to the order. Add. p. 13. Although the court issued an order that at least arguably bound mirror sites

³ These facts illustrate that in appellants’ view the factual findings of the court were clearly erroneous. However, by refusing to hear contrary facts, the

court erred as a matter of law. If further proceedings are held, and appellants given an opportunity to be heard, and the court made findings on a contested record, then the question of whether the findings were clearly erroneous will be presented.

such as appellants, it did not even discuss possible harm to them. Suppression of speech by non-consenting speakers such as appellants is classic irreparable harm. Elrod v. Burns, 427 U.S. 347, 373 (1976). The court's factual finding was possible only by ignoring the interests of appellants (while at the same time arguably enjoining their speech).

Moreover, the finding concerning the harm to the public is extremely suspect. The code written by Jansson/Skala and mirrored by appellants is analogous to a key that unlocks the Cyber Patrol blocked sites list. However, Cyber Patrol has changed the lock. Any owner may download the new lock so that the key no longer works. App. p. 98. In addition, Cyber Patrol is a product that blocks access to web pages. It has blocked access to all of the "mirror" sites. Thus, lawful owners of Cyber Patrol cannot go to those pages to get the key. Id. Cyber Patrol argued that the children whose parents had installed Cyber Patrol on their home computer and who went onto

the Jansson/Skala web site and downloaded their computer code, could have a method to access blocked sites. App. p. 11, ¶14. Clearly the concern that children would be unprotected was a prime consideration in the district court's order. Add. p. 17-18. However, Cyber Patrol had already eliminated that danger.

The district court rejected the defense of "fair use." Add. pp. 11-12. That

was legal error. See section V, infra. It was also based on one-sided factual findings that, if evidence had been allowed, would have been shown to be wrong.

Jansson and Skala capitulated to the settlement demands of Cyber Patrol (apparently to avoid financial ruin⁴), and agreed to every finding of fact and conclusion of law that Cyber Patrol asked them to sign off on. Thus, the court never heard facts (other than those of Cyber Patrol) on the issue of whether the creation of their computer code was protected under the fair use doctrine. The district court merely observed that "[t]he individual defendants have no 'fair use' defense here because they have neither asserted it nor submitted evidence supporting any fair use defense." Add. p. 11, ¶47. Appellants had, of course, asserted the defense but were

refused the right to submit evidence. App. p. 3, docket entry 9 (Opposition to Motion for Preliminary Injunction).

However, the district court also found that fair use was unavailable because "the copying here is inconsistent with the general public good." Add. p. 11-12, ¶48. Appellants were denied the opportunity to present facts on this question prior to the issuance of the injunction.

⁴ Defendant Skala wrote: "I faced a very tough decision as to how aggressively to attempt to fight it. On the one hand, I believe that what I did was legal and right. It goes against my grain to allow Mattel or anybody else to intimidate me. On the other hand, I didn't have a lot of resources to fight with. I'm just a student myself, not a multi-billion-dollar company."
www.islandnet.com/~mskala/cpbfaq.html

First, appellants would have provided evidence about the importance of reverse engineering generally to software analysis and the value for criticism and for creating interoperable programs (i.e. programs that will work with other programs). Reverse engineering of software programs is a necessary prerequisite to discovering uncopyrightable information about how the program works. In this case, it would show what sites the program blocked. Reverse engineering of software that you already own is analogous to taking apart your car to see how it works.⁵ No evidence

on this was presented to the district court. App. pp. 7-40, 57-81.

Appellants would have presented evidence on the importance for owners (or prospective owners) of Cyber Patrol and the general public of knowing the sites that are blocked. As indicated above, products such as Cyber Patrol have been enormously controversial. One of the central controversies has been over the degree to which such products work, that is, do they successfully block “offensive” sites but leave accessible useful sites. Evidence would show that there

⁵ Defendant Skala described his motive for creating the code in similar terms. “I think it's important for people to think about the issues related to censorware, and it's hard to have an informed debate without knowing what the products actually block. So that's one reason to make the blocking list available. Another reason would be consumer protection - if teachers, librarians, employers, and parents are considering buying this kind of software, they have a right to know what they're getting. If the manufacturer won't tell them what the product does, it's appropriate for someone else to do that; in much the same way that Consumer Reports publishes information about vehicle safety hazards.”
www.islandnet.com/~mskala/cpbfaq.html

is considerable reason to doubt the effectiveness of such products generally and Cyber Patrol in particular. Cyber Patrol blocks or has blocked (as sexually explicit) web pages of the Ontario Center for Religious Tolerance, the HIV/AIDS Information Center of the Journal of the American Medical Association (JAMA), the University of Newcastle's computer science division, Nizkor (a Holocaust remembrance site), Nike shoes, the National Academy of Clinical Biochemistry, the U.S. Army Corps of Engineers, the MIT Student Association for Free Expression, Planned Parenthood, and the Electronic Frontier Foundation (a public interest law group that was among the counsel for plaintiffs in Reno v. ACLU). Because the lists are kept secret, it is often difficult to establish which sites are blocked. In Mainstream Loudoun, discovery made it possible to learn some of the sites blocked by a competitor of Cyber Patrol. In addition to the sites mentioned in the Statement of the Case above, that product blocked as sexually explicit the Quakers; the National Journal of Sexual Orientation Law; the AIDS Quilt Info & Links; the Heritage Foundation; Fairness and Accuracy in Reporting; Community United Against Violence; the Glide Memorial Methodist Church; the Center for Reproductive Law and Policy; the entire web site of the San Francisco Chronicle; a bibliography of psychiatry, madness and insanity; the Wesleyan University Philippines Mass Communication Society; and several personal home pages, including a personal page containing photos of National Parks. Moreover, the evidence in that case showed that this "overblocking" was

an inescapable fact of these products given the size of the Internet and the rate at which it changes.⁶ Moreover, the evidence would also show that products such as Cyber Patrol do not succeed in blocking all sites that are sexually explicit.⁷

The Jansson/Skala speech assisted owners of Cyber Patrol in learning more about the blocked sites list. Surely, it is in the “public interest” for owners to know about blocked sites when deciding to purchase any such product or when deciding to purchase Cyber Patrol rather than one of its competitors. Perhaps the district court’s factual finding that “fair use” was inapplicable because disclosure was not in the public interest would have been different had it allowed facts critical of Cyber Patrol’s views to be presented.

Appellants would have also presented evidence that the harm to Cyber Patrol, if any, from publication of the code and/or the blocked sites list was minimal and far outweighed by the benefits to both parents and to the underlying policy debate.

⁶ These facts are found on www.peacefire.org (run by one of appellants), www.censorware.org, and www.aclu.org/courts/loudoun_brief; See also Jonathan Weinberg, “Rating the Net,” 19 Comm/Ent 453, 459-470 (1997).

⁷ Defendant Skala said: “we found considerable evidence of poor quality control. We found some evidence of Web sites that may have been added to the list by automated searches without human review. We found a great many sites that were blocked under their former but not current addresses, suggesting that blocks are not reviewed once added. We found some categories that had apparently been applied overly broadly...”
www.islandnet.com/~mskala/cpbfaq.html.

The district court justified its decision to apply the injunction to those “in active concert” because of another key factual issue. The court concluded that “[m]any of the persons who created the mirror sites did so” in order to prevent the court from awarding meaningful relief to the plaintiff. Add. p. 4, ¶15. The court based this finding on representations of plaintiff’s counsel that appellants were never permitted to dispute; plaintiff submitted an affidavit by counsel asserting that appellants were “in privity” with Jansson/Skala and therefore “in active concert.” App. p. 62, ¶3.⁸ One piece of Cyber Patrol’s submission not mentioned by counsel and apparently not noticed by the court contradicted that representation by counsel. App. p. 33. And, if appellants had been able to present evidence, it would have showed that many of the mirror sites were created for the purpose of disseminating information about Internet filtering programs and their weaknesses, and without regard to the judicial proceeding.

Under the procedures adopted by the district court, it is possible that appellants will be able to argue the facts relevant to the “active concert” issue (though not to any other issues in the case). However, they may do so only if they risk contempt and if Cyber Patrol files a contempt motion.

⁸ The sole basis for counsel's assertion was that appellants “copied the content [of defendants’ speech] directly from [defendants’] Web page or from

someone else who did so” allegedly “for the avowed purpose of seeking to avoid” the TRO in this case. App. p. 62, ¶3. Even if these facts were assumed to be true, they do not establish any connection between Jansson/Skala and appellants that would constitute “privity” or would justify binding appellants under Rule 65(d).

In justifying extension of the order to those “in active concert,” and denying appellants the right to present evidence on the validity of the underlying order, the district court relied on and utilized the language of Fed. R. Civ. Pro. 65(d). Appellants, of course, have no quarrel with Rule 65(d) which is properly designed to prevent a party from using another to achieve indirectly what the party has been prohibited from achieving directly. However, even if appellants had been “in active concert” with Jansson/Skala (which there are no facts to support), Rule 65(d) cannot

be used to prevent appellants from challenging the validity of the order. Appellants sought to challenge the validity of the order on a timely basis. Indeed, appellants argued, prior to entry of the settlement order, that the facts on which it was based were wrong. App. p. 3, docket entry 9, Opposition to Motion for Preliminary Injunction. Under these circumstances, appellants should have been allowed to present facts to challenge the validity of the order. See National Wildlife Federation v. Gorsuch, 744 F.2d 963 (3rd Cir. 1984) (untimely failure to raise claims when given the opportunity precludes subsequent litigation of those claims).

An analogy vividly illustrates this point. Assume that Cyber Patrol had settled with respect to Jansson, who agreed to an injunction, and further agreed it would bind those “in active concert.” Assume further that Skala had refused to

settle and sought to contest personal jurisdiction, subject matter jurisdiction, and the legality of his actions. There can be no doubt that Skala was “in active concert” with Jansson. Could Cyber Patrol have dismissed the case as to Skala but taken the position that Skala was bound by the settlement order it obtained from Jansson? By doing so, could Cyber Patrol forever foreclose the opportunity of Skala to raise all of his defenses? Yet, that, in effect, is what did occur in this case. Appellants have been effectively bound by the order and precluded forever from raising defenses that they sought on a timely basis to raise.

Rule 65 does not permit this procedure. If appellants could have but did not seek to raise their defenses on a timely basis and at some later date were shown to be in “active concert” with Jansson/Skala, Rule 65(d) would bind them and could limit the defenses they could then raise. But that is not this case and the procedure adopted by the district court violated due process.

IV. THE DISTRICT COURT DID NOT HAVE JURISDICTION TO ENTER THE STIPULATED PERMANENT INJUNCTION.

The district court held that it had subject matter jurisdiction under 28 U.S.C. §1338, which grants federal district courts exclusive jurisdiction over "any civil action arising under any Act of Congress relating to patents, plant variety protection, copyrights and trade-marks." Add. p. 6, ¶27. Cyber Patrol's complaint alleged that Jansson/Skala engaged in acts of reverse engineering of Cyber Patrol's program in Canada and in Sweden, in willful violation of the U.S.

Copyright law. App. p. 9-10. In addition, Cyber Patrol's complaint alleged the Jansson/Skala may have obtained an unlicensed copy of Cyber Patrol's program in Canada or Sweden, and used that unlicensed copy in Canada or Sweden, in violation of U.S. copyright law. App. pp. 9-11. Finally, the complaint alleged, Jansson/Skala used information they discovered in the course of the reverse engineering process to create and post on the Internet a program capable of disabling particular features of plaintiff's program. App. pp 10-

11. That program was not alleged to contain any infringing code from Cyber Patrol's program. Id. As argued below, none of these acts would have violated U.S. copyright law if they had occurred within the United States. Because all of the allegedly infringing acts were committed in Canada or Sweden, however, the United States copyright law does not even apply to this dispute.

U.S. copyright laws have no extra-territorial application. E.g., Twin Books Corp v. Walt Disney Co, 83 F.3d 1162, 1166-67 (9th Cir. 1996); Update Art v. Modiin Publishing, 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. 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)) . 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, Los Angeles News Service v. Reuters Television International, 149 F.3d 987, 990-92 (9th Cir. 1998), 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.

The sole activity alleged to have occurred in the U.S. is that Jansson/Skala bragged about their 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. App. p.11, ¶¶16-17; Add. p. 2-3, ¶¶7, 10. 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.

The court nonetheless held that it could exercise jurisdiction because "[w]hen an allegedly infringing act occurring outside the United States is transmitted into the United States, the Copyright Act is implicated and a district court possesses jurisdiction." Add. p. 6, ¶28. That is not the law. 13 U.S.C. § 1338 does not grant the federal district courts jurisdiction over any civil action that implicates the U.S. Copyright Act, but only over those actions that *arise under* federal copyright statutes. The foreign use of an unauthorized copy of a

work, and foreign reverse-engineering of a work simply do not give rise to an action under the federal copyright statute.

The district court cited National Football League v. TVRadio Now Corp., ___F.3d ___, 53 U.S.P.Q. 2d 1831 (WD Pa 2000), Los Angeles News Service v. Conus Comm. Co., 969 F. Supp. 579, 583-84 (CD Cal. 1997) and Metze v. May Department Stores, 878 F. Supp. 756, 761 (WD Pa. 1995) in support of its conclusion. Add. p. 6, ¶28. None of those cases offers support for the exercise of subject matter jurisdiction in this case. In NFL v. TVRadio Now, plaintiff alleged that defendant captured copyrighted performances broadcast in Buffalo NY, converted those performances into computer data in Canada, and then transmitted those performances to computers throughout the United States, thus publicly performing plaintiffs' copyrighted programs within the United States, in violation of 17 U.S.C. §106(4). See 53 USPQ 2d at 1834-35. Similarly, in Los Angeles New Service v. Conus Co., defendant broadcaster transmitted plaintiff's copyrighted programming into the United States. The court found subject matter jurisdiction on the basis of unlawful public display of the material within the United States in violation of 17 U.S.C. § 106(5). 969 F. Supp. at 583-84. In Metze v. May Departments Stores, defendant arranged for a Taiwanese company to make infringing copies of plaintiff's work, imported those copies, and displayed and distributed them in the United States. The court rejected May's claim that its liability should be limited to copies distributed by it within the US

and should not extend to copies made abroad at its behest and distributed by unrelated companies within the U.S. 878 F. Supp. at 758-61. In all three cases, the courts based their exercise of federal subject matter jurisdiction on the illegal distribution, performance or display of copies of plaintiff's copyright work within the United States. See also National Football League v. Primetime 24 Joint Venture, 2000 U.S. App. LEXIS 8275 (2d Cir. 2000) (unauthorized transmission of plaintiff's copyrighted material from the US to Canada is a public performance within the United States in violation of §106(4)).

The district court concluded that Jansson/Skala violated the U.S. copyright statute "by sending by email their press release into the United States and encouraging United States citizens to obtain copies of the Bypass Code [the code written by Jansson/Skala] by downloading or replicating it into the United States." Add. p. 8, ¶31. Neither the press release nor the Bypass Code, however, were alleged to contain copyright protected code from Cyber Patrol's program. Rather, Cyber Patrol alleged that solely because they were created using information obtained through acts that it claimed would have violated the U.S. copyright law if they had been committed within U.S. borders, those works themselves violated the copyright. That is also not the law; the U.S. copyright statute has no "fruit of the poisonous tree" doctrine. If the material transmitted into the United States was not an unlawful copy of Cyber Patrol's program, and there was no allegation that it was, then the claim that it was created using

unlawfully obtained information does not convert it into a copyright violation. The district court's exercise of subject matter jurisdiction under 28 U.S.C. § 1338 was therefore improper.

Without subject matter jurisdiction over the complaint, the district court had no authority to enter the permanent injunction.

The distinction between subject-matter jurisdiction and waivable defenses is not a mere nicety of legal metaphysics. It rests instead on the central principle of a free society that courts have finite bounds of authority, some of constitutional origin, which exist to protect citizens from the very wrong asserted here, the excessive use of judicial power. The courts, no less than the political branches of the government, must respect the limits of their authority.

United States Catholic Conference v. Abortion Rights Mobilization, Inc., 487 U.S. 72, 77 (1988). See also Update Art, 843 F.2d at 72 ("subject matter jurisdiction is a constitutional prerequisite to a federal court's power to act").

V. EVEN IF THE COURT HAD SUBJECT MATTER JURISDICTION, THE U.S. COPYRIGHT LAW WOULD HAVE PERMITTED JANSSON/SKALA TO MAKE A COPY OF CYBER PATROL UNDER THESE CIRCUMSTANCES.

A. Fair Use

Even if Jansson/Skala made a copy of Cyber Patrol as a predicate for writing their own code, and even if U.S. law applied, the copying would still be legal because it constituted "fair use" under 17 U.S.C. § 107. Fair use is a fundamental principle of copyright law, firmly embedded in the Copyright Act itself and with a rich history as a protector of free speech against the potential anticommunicative impact of intellectual property laws. As stated by Congress:

[Th]e fair use of a copyrighted work . . . for purposes such as criticism, comment, news reporting, teaching . . ., scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is fair use, the factors to be considered shall include —

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

17 U.S.C. § 107. None of these factors is dispositive; rather, they are to be weighed together.

This Court need not reinvent the wheel in its effort to determine whether the making of an intermediate copy of copyrighted software for purposes of reverse engineering it and creating compatible applications constitutes “fair use.” Several courts have already held that it does, including a recent, much-awaited Ninth Circuit decision on the subject. See Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596, 603 (9th Cir. 2000). Reverse engineering, as these courts have recognized, serves important social and economic functions, including making available to the public software that is complementary to, or interoperable with, existing software.

That is precisely what the Jansson/Skala software does: It permits a parent, for example, who has purchased the Cyber Patrol software to determine whether that product effectively does what it is advertised as doing, and to determine what sites the buyer's children will be blocked from seeing if and when the parent chooses to activate the software on a particular computer. The evidence — had the court permitted evidentiary hearings prior to entry of a permanent injunction that purportedly binds the appellants — would undoubtedly show that reverse engineering the Cyber Patrol program was necessary in order to discover uncopyrightable information about how the program worked and what sites it blocked.

In sum, as other Circuits have already held, reverse engineering software to create interoperable or compatible applications constitutes “fair use” even though it involves the creation of an intermediate copy of the copyrighted work. See, e.g., Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596, 603 (9th Cir. 2000); Sega Enter. 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). As the Ninth Circuit recently explained in Connectix, “[the] unprotected ideas and functions of [computer software code] are frequently undiscoverable in the absence of investigation and translation that may require copying the

copyrighted material.” 203 F.3d at 602. Accordingly, “intermediate copying and use of Sony’s copyrighted [code] was a fair use...” Id.

Ironically, Cyber Patrol, in the conclusions of law drafted for and adopted by the district court, cited the Connectix case for the proposition that creating an intermediate copy is a prima facie copyright violation. Add. p. 11, ¶ 43. However, the Ninth Circuit had gone on to find that the use was “fair” and therefore noninfringing, a holding not brought to the district court’s attention by Cyber Patrol and not cited in the conclusions of law. Connectix, 203 F.3d at 602-10.

To avoid a fair use analysis, Cyber Patrol offered the court a simple solution, which it adopted: There was no need to consider “fair use” because the individual named defendants, Jansson and Skala, “neither asserted it nor submitted evidence supporting any fair use defense.” Add. p. 11, ¶47. That conclusion may be true as to Jansson/Skala, but obviously cannot be so as to appellants who did attempt to assert the “fair use” defense and were not allowed to present evidence. See section III.B, supra.

As a matter of law, the actions undertaken by Jansson/Skala in furtherance of their efforts both to prove the lack of security in Cyber Patrol and to expose and discuss the nature of the specific web sites censored by Cyber Patrol’s software constitute the sort of public commentary and criticism that is at the core of “fair use” and indeed essential to the vibrant dissemination of opinions in a

free society. As explained in Sega, and reiterated in Connectix:

[W]here disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law.

Connectix, 203 F.3d at 602, (quoting Sega, 977 F.2d at 1527-28) (emphasis altered). Notably, the uses for which disassembly was necessary in Connectix and Sega were purely commercial — the defendants wished to release products competitive and compatible with those sold by plaintiff. Here, the purpose is noncommercial: Jansson/Skala wished (until entry into the settlement) to comment — and appellants still do — on the nature of “censorware” such as Cyber Patrol. If the public’s desire for cheaper video games is a sufficient social purpose to overcome the copyright protection in the intermediate copy, surely the dissemination of knowledge as to what types of web sites are being blocked from children by popular censorware, and indeed the knowledge as to whether those products even work properly, is a far clearer example of “fair use.”

In sum, Connectix makes it clear that this type of reverse engineering is protected as “fair use.” An independent analysis of the four “fair use” factors in the

context of this case, moreover, confirms the principle that reverse engineering — at least on the facts of this case — is “fair use.”⁹

As an initial matter, the preamble to Section 107 identifies “criticism” as one of the categories of “fair use.” The Jansson/Skala work is indisputably criticism. It contained critical commentary on, as well as a demonstration of the ineffectiveness of Cyber Patrol.

The first Section 107 factor, the “purpose or character of the use,” looks to whether the use is commercial, on the one hand, or educational, critical, social or political, on the other. See, e.g., Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 562 (1985); American Geophysical Union v. Texaco, Inc., 60 F.3d 913 (2d Cir. 1995). The Jansson/Skala code falls squarely in the second category. The code is not sold, but rather is given away for free as a socio-political statement; indeed, its availability is unrelated to any commercial venture or operation whatsoever. Rather, as evidenced both by their own commentaries and those of numerous “mirror” sites, including appellants, who chose to post their code,

⁹ The district court largely refused to engage in this analysis because it believed that it did not have to. Add. p. 11, ¶47. Instead, it relied primarily on generalizations about the value of Cyber Patrol. See e.g. Add. pp. 11-12, ¶48 (“general public good”); Add. p. 13, ¶53 (“public...will suffer...harm”); Add. p. 17-18 (societal importance of Cyber Patrol). As noted above, those generalizations were expressly contested by appellants and due process required that appellants be able to present evidence that they were wrong. As suggested in this section, this Court could engage in the statutory analysis and conclude as a matter of law that fair use occurred.

Jansson/Skala's purpose, much like appellants', was to expose both the weaknesses or failures of the Cyber Patrol and comparable "censorware" products in living up to their stated purpose and, more fundamentally, to expose and comment critically upon Cyber Patrol's selective list of censored web sites, many of which parents or educators would probably be surprised to learn that their children are being denied access to. Whether one agrees with the views of Jansson/Skala and appellants on this issue or not, what remains undeniable is their First Amendment right to express them, and the fact that, accordingly, their conduct lies at the core of what "fair use" is all about.¹⁰

The second factor, the "nature of the copyrighted work," acknowledges that "some works are closer to the core of intended copyright protection than others." Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 586 (1994). This factor thus looks to whether the work lies on the expressive end or the factual/functional end of

the spectrum of copyrightable works. Undeniably, software is considered a work of authorship that can be entitled to copyright protection. Junger v. Daley, 209 F.3d 481 (6th Cir. 2000). But within the range of protectable works, some are

¹⁰ Enjoining the publication of an original work of authorship (in this case computer code) that reveals the weaknesses, deficiencies, and political biases of a popular software product is a classic prior restraint on speech in violation of the First Amendment. In Harper & Row, the Supreme Court cautioned against allowing an "abuse of the copyright owner's monopoly as an instrument to suppress facts." 471 U.S. at 559.

particularly expressive and therefore allow only much more rarely for any finding that a copy can be “fair use.” Others, by contrast, are largely factual or functional in nature, and as to such works it is much easier to find their copying to be “fair use.” Software is functional: it is not meant to be art or literature; it is meant to implement an algorithm that achieves a particular result. It thus “contains unprotected aspects that cannot be examined without copying.” Connectix, 203 F.3d at 603. The second factor, accordingly, also favors appellants.

The third fair use factor examines the amount or substantiality of the use. There has been no evidence of the amount copied. Even if, as in most reverse engineering cases, the entire code were copied, that would not preclude a finding of fair use. “[I]n a case of intermediate infringement when the final product does not itself contain infringing material, this factor is of ‘very little weight.’” Connectix, 203 F.3d at 606, (quoting Sega, 977 F.2d at 1526-27). See also Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 449-50 (1984) (copying of entire work does not preclude fair use). Moreover, as discussed above, it must be recalled that this entire analysis is directed at whether the party making the “intermediate copy” engaged in infringement or fair use. Appellants are not that party. There is no allegation that appellants themselves (the operators of mirror sites) copied anything belonging to Cyber Patrol. This case is thus far stronger than Connectix (which itself found fair use).

The fourth and final “fair use” factor is the impact on the market. This factor looks to whether there is a market for defendant’s work that substitutes for the market for plaintiff’s work. If a defendant copies and sells a popular novel, for example, that act plainly diminishes the market for the novel as sold by the copyright owner. The district court found that the Jansson/Skala code would diminish Cyber Patrol’s market largely because the code illustrated flaws in the product. Add. pp. 12, ¶¶49-50. But the Supreme Court has made it clear that this factor is not meant to be used as a license to target and chill criticism. See Campbell, 510 U.S. at 591-92 (“[W]hen a lethal parody, like a scathing theater review, kills demand for the original, it does not produce a harm cognizable under the Copyright Act.”). A devastating critique may well diminish the market for a work, but does not thereby undermine the reviewer’s “fair use” right to quote from the book in the course of writing and publishing the review. In this case, analogously, the only detriment to Cyber Patrol’s market (even assuming it had adduced evidence of lost sales or other damage or detriment, which it did not) would derive from the critical nature of the appellants’ speech — i.e. the fact that it exposes weaknesses in Cyber Patrol and discloses information about which web sites are blocked and which are not. That form of “impact on the market” is not one that fair use law permits the courts to consider. Plainly, the Janssen/Skala code does not substitute in the marketplace for Cyber Patrol — its

purpose is utterly at odds with Cyber Patrol's. Accordingly, the fourth fair use factor favors appellants as well.

As many courts have noted, a “transformative work” — one that does not merely supplant or supersede the original work but rather creates a new and different product — is less likely to have an adverse impact on the market for purposes of factor four. Harper & Row, 471 U.S. at 567-69; Connectix, 203 F.3d at 607; Texaco, 60 F.3d at 930. Here, the purpose of the intermediate copying was “transformative,” *i.e.* served a function substantially different from that of the original work. Jansson/Skala did not copy Cyber Patrol in order to sell a competing product. Any “intermediate copying” of the Cyber Patrol code was in service of their transformative purpose to produce an entirely different, albeit interrelated, piece of software and critical commentary.

In sum, both as a matter of precedent and in light of the analysis of the four fair use factors set forth above, Janssen/Skala's copying, even if it had been committed in the United States and were thus subject to the jurisdiction of the court, constituted “fair use.” *A fortiori*, the mirroring of that information on the web sites of appellants, who are not alleged to have made any infringing “intermediate copies” at all, cannot be infringement.

B. License Agreement

Nor can Cyber Patrol circumvent this problem by claiming breach of the Cyber Patrol license agreement. The district court found that Microsystems

distributes Cyber Patrol “subject to” a license agreement. Add. p. 2, ¶4. But it did not find, and Cyber Patrol has neither alleged nor proven that Jansson/Skala entered into any such license agreement. App. p. 10, ¶10. Perhaps more to the point for purposes of this appeal, there is no allegation or evidence that appellants signed or otherwise expressly or impliedly entered into any such license agreement.

It is far from clear that mass market “license” agreements purporting to bind the user of software to terms that prohibit reverse engineering and other fair use are legally enforceable. While the Seventh Circuit has held that some so-called shrink-wrap agreements are, in some circumstances, enforceable, see ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), other courts (as well as numerous commentators) have rejected that approach and suggested that such agreements are preempted by federal copyright law. See, e.g. Vault Corp. v. Quaid, 847 F.2d 255 (5th Cir. 1988).¹¹ See also M. Lemley, Intellectual Property and Shrink Wrap Licenses, 68 S. Cal. L. Rev. 1239 (1995).¹²

¹¹ In Vault, the court noted that Section 117 of the Copyright Act sets forth situations in which the owner of a computer program may make an adaptation of

that program, and by doing so evidences Congress’s intent to occupy that field and preempt state law that would allow contrary provisions. Accordingly, a “license agreement against decompilation or disassembly is unenforceable.” Id. at 270.

¹² The validity of shrink wrap licenses in Massachusetts is unresolved. Cf. Green Book Int’l v. InUnity Corp, 2 F. Supp. 2d 112 (D. Mass. 1998)(not reaching the issue).

Whether this Court, in an appropriate case, would follow the Seventh Circuit's or the Fifth Circuit's approach on this issue need not be resolved at this time. Cyber Patrol has made no showing, and the district court has made no finding, that Jansson/Skala entered into such an agreement, or that it is enforceable under the laws of whatever country (presumably Sweden or Canada) that they may have entered into it in. More importantly, there has been no allegation or showing that appellants entered into, or are in any way bound by, any such agreement. Leaving aside the serious doubts surrounding the validity of "shrinkwrap" and "clickwrap" licenses,¹³ it is elementary that they do not bind persons, such as appellants, who are not alleged to have unwrapped, clicked, signed, or even seen such an agreement.

CONCLUSION

For all these reasons, appellants respectfully ask that the district court's order entering the stipulated permanent injunction be reversed and the injunction vacated in full.

Respectfully submitted,

¹³ Cyber Patrol does not indicate which type of agreement is at issue here or how any party (or nonparty) manifested its assent to the terms of the agreement.

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

Sarah R. Wunsch, # 28628
American Civil Liberties Union Fdn.
of Massachusetts
99 Chauncy Street, Suite 310
Boston, Massachusetts 02111
(617) 482-3170, ext. 323

Of counsel:
David L. Sobel
Electronic Privacy Information Center
1718 Connecticut Ave, NW Suite 200
Washington D.C. 20009
(202) 483-1140

Jessica Litman
Professor of Law
Wayne State University
468 West Ferry Mall
Detroit, MI 48202
(313) 577-3952

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. Pro. 28(a)(11), the undersigned certifies that this brief, exclusive of the exempted portions, contains 12,345 words. The brief has been prepared in proportionally spaced typeface using: WP 8; Times New Roman, 14 point .

Dated: June 6, 2000

Christopher A. Hansen

CERTIFICATE OF SERVICE

I, Christopher A. Hansen, hereby

certify that on this the 6th day of June, 2000, a correct copy of the Brief of the Appellant was served via Federal Express upon the following parties:

Irwin B. Schwartz
Joel G. Beckman
Laura N. Kling
Schwartz and Nystrom, LLC
419 Boylston Street
Boston, MA 02116

and by U.S. Mail to the following:

Edmund Letain
Cardinal, Emberton, Rusk & Carfra
2787 Jacklin Rd.
Victoria, British Columbia
V9B 3X7

Ulf Svalling
Careligatan 7A
SE-632 20 Eskilstuna
Sweden

Christopher A. Hansen