

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

-----  
---

MICROSYSTEMS SOFTWARE, INC., a  
Massachusetts corporation,  
and MATTEL, INC., a Delaware  
corporation,

Plaintiffs,

vs.

SCANDINAVIA ONLINE AB, a Swedish  
corporation; ISLANDNET.COM, a  
Canadian corporation; EDDY L. O.  
JANSSON, a Swedish citizen; and  
MATTHEW SKALA, a Canadian  
citizen,

Defendants.

-----  
MEMORANDUM IN SUPPORT  
OF EX PARTE MOTION FOR  
TEMPORARY RESTRAINING  
ORDER AND  
EXPEDITED DISCOVERY

Plaintiffs Microsystems Software Inc. and Mattel, Inc.  
(together, "Microsystems") respectfully submit this memorandum  
in support of their Ex Parte Motion For Temporary Restraining  
Order and Expedited Discovery.

INTRODUCTION

Defendants Eddy L. O. Jansson and Matthew Skala  
("Jansson" and "Skala", respectively) violated Federal and  
international copyright protections by reverse engineering  
Microsystems' Cyber Patrol child-protection software.  
Jansson and Skala then created and posted on their Web sites,  
hosted by defendants Scandinavia On Line AB ("Scandinavia  
Online") and Islandnet.Com ("Islandnet"), source code and  
binaries designed to bypass Cyber Patrol (the "Bypass Code").  
These Web sites allow children to download the Bypass Code and  
defeat their parents' efforts to screen out sexually explicit  
and other Web content inappropriate for children such as  
materials advocating drugs, violence, explosives or cults.

The Bypass Code created in violation of Microsystems' copyrights is distributed on the World Wide Web and is causing Microsystems immediate and irreparable harm. Moreover, the Bypass Code posted on the defendants' Web sites potentially exposes thousands of children to material on the Internet that their parents affirmatively sought to screen out.

Accordingly, Microsystems respectfully requests that the Court: (1) temporarily restrain all defendants and order defendants to take down the links to Jansson's and Skala's Web sites posting the Cyber Patrol Bypass Code and binaries, and to enjoin defendants from further disseminating such information; (2) permit Microsystems extremely limited expedited discovery to further identify Jansson and Skala as well as to track identities and addresses of all persons who accessed the Bypass Code; and (3) order the defendants to preserve all documents and data in their present form and keep inviolate the Bypass Code contained on Jansson's and Skala's Web sites.

#### FACTS

Microsystems developed and markets and licenses Cyber Patrol software, which is designed to screen computer access to sexually explicit and other materials posted on the Internet (Ver. Comp. 1). Microsystems holds registered copyrights in the Cyber Patrol software program (Ver. Comp. 8). Anyone lawfully obtaining a copy of Cyber Patrol is required to agree to explicit prohibitions against reverse engineering the software as provided in the Cyber Patrol software license agreement:

This is a legal agreement between you (either as an individual or an entity) and Mattel, Inc. BY INSTALLING OR USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, AND YOU ARE THE ORIGINAL PURCHASER OF THE SOFTWARE, PROMPTLY UNINSTALL THE SOFTWARE FROM YOUR HARD DRIVE OR RETURN THE SOFTWARE (INCLUDING PRINTED MATERIALS) TO THE PLACE WHERE YOU PURCHASED IT FOR A FULL REFUND.

**COPYRIGHT.** All intellectual property rights in the Software (including all animations, audio, images, maps, music, photographs, video, and text incorporated into the Software) are owned by Mattel, Inc. and its affiliates, suppliers, and licensors, and are protected by United States copyright laws and international treaty provisions . . . You may not reverse engineer, decompile, or

disassemble the Software, except to the extent that this restriction is expressly prohibited by applicable law. (Ver. Comp. 9). Jansson and Skala obtained a copy of Cyber Patrol software either by piracy or under the license agreement (Ver. Comp. 10).

After obtaining a copy of Cyber Patrol, Jansson and Skala willfully, knowingly and deliberately undertook to violate Microsystems' copyrights in the software (Ver. Comp. 21). Jansson and Skala openly admit that they reverse engineered Cyber Patrol notwithstanding the express prohibitions in the license agreement (Ver. Comp. 12). Thereafter, again by their own admission, Jansson and Skala used the information they obtained by reverse engineering to develop the Bypass Code (Ver. Comp. 14). Jansson and Skala then posted links on their respective Web sites to enable Internet users to download the Bypass Code (Ver. Comp. 15).

On March 11, 2000, Jansson and Skala issued a press release bragging that they had reverse engineered the Cyber Patrol software and posting the Web address at which users could download for free the Bypass Code (Ver. Comp. 16). In their press release, Jansson and Skala announced: CyberPatrol(R)4, a "censorware" product intended to prevent users from accessing undesirable Internet content has been reverse engineered by youth rights activists Eddy L. O. Jansson and Matthew Skala. A detailed report of their findings, titled, "The Breaking of Cyber Patrol(R)4", with commentary on the reverse engineering process and cryptographic attacks against the product's authentication system, has been posted on the World Wide Web . . . A package of source code and binaries implementing the attacks is included.

(Ver. Comp. 16). Jansson and Skala sent their press release via E-mail to individuals and organizations throughout the United States and the world, including a web-hosting service in Acton, Massachusetts (Ver. Comp. 17).

The practical effect is that, through Jansson's and Skala's Bypass Code promotion and Internet posting, children may bypass their parents efforts to screen out inappropriate materials on the Internet (Ver. Comp. 18).

#### ARGUMENT

##### I. Microsystems is Entitled To Injunctive Relief

A temporary restraining order or preliminary injunction should issue where there has been a copyright violation. 17 U.S.C. § 502(a). See *Accusoft Corp. v. Palo*, 923 F. Supp. 290, 297 (D. Mass. 1996) (issuing injunction pursuant to 17 U.S.C. § 502(a) and Fed. R. Civ. P. 65(d) in copyright dispute). Courts apply a modified injunctive relief standard

in copyright cases and the movant need only show two factors: likelihood of success on the merits and that the balance of harms tips in its favor. *Id.* at 295 (citation omitted).

A.       Microsystems Is Likely To Succeed On The Merits Of Its Copyright Infringement Claim

To prove a copyright violation, Microsystems need only demonstrate (1) ownership of a valid copyright and (2) copying by the defendants. *Data General Corp. v. Grumman Systems Support Corp.*, 803 F. Supp. 487, 490 (D. Mass. 1992) (denying motion to dismiss copyright violation); *Accusoft Corp.*, 923 F. Supp. at 295 (reciting elements of copyright claim).

"[I]ntermediate copying of computer object code may infringe exclusive rights granted to the copyright owner". *Sega Enter.*, 977 F. Supp. at 1519.

In this case, there can be no dispute that Microsystems has a valid copyright in *Cyber Patrol* (Ver. Comp. 8). In addition, Jansson and Skala have admitted that they reversed engineered Microsystems' copyrighted work, which is a prima facie violation of the copyright laws (Ver. Comp. 12, 13). In fact, defendants Jansson and Skala either unlawfully obtained the *Cyber Patrol* software in the first place or obtained it by license which they then violated by the reverse engineering process (Ver. Comp. 10). In either case, the defendants have violated Microsystems' copyright. See *Sony Computer Enter.*, 2000 WL 144399 at \*6; *Sega Enter.*, 977 F.2d at 1518.

B.       The Fair Use Exception Is Inapplicable Here

To establish that a copyright violation is permitted by the fair use exception, courts weigh the following four statutory factors:

(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.

As the Ninth Circuit held in *Sony Computer Entertainment, Inc. v. Connectix Corp.*, and *Sega Enter. LTD. v. Accolade, Inc.*, Jansson and Skala's disassembly of copyrighted object code was, as a matter of law, a fair use only under narrow

exceptions. *Sony Computer Enter.*, 2000 WL 144399 at \*6; *Sega Enter.*, 977 F.2d at 1518. The narrow exception carved out by the Ninth Circuit is inapplicable here because Jansson and Skala can claim no "protected by copyright" or some other such "legitimate reason" for reverse engineering. *Sega Enter.*, 977 F.2d at 1518. Rather, Jansson and Skala were accessed Microsystems' copyrighted code in with the purpose to destroy its usefulness and cause irreparable harm to Microsystems. This conduct does not fall into the narrow exception carved out by the Ninth Circuit.

Furthermore, to "negate fair use one need only show that if the challenged use should become widespread, it would adversely affect the potential market for the copyrighted work." *Harper & Row, Pub. Inc., v. Nation Ent.*, 417 U.S. 539, 568 (1985) (finding no fair use). By their own admission, Jansson and Skala created the Bypass Code to "break" Cyber Patrol (Ver. Comp., Ex. A). Software explicitly designed to make Cyber Patrol ineffective for its intended use, by definition, seeks to destroy the market for Microsystems' product.

Moreover, the fair use exception is unavailable here because the express purpose of the Bypass Code is contrary to Congressional intent. The fair use exception cannot be used to protect work that expressly violates public policy.

C. The Harm To Microsystems Outweighs  
Any Possible Harm to Defendants

An injunction should enter where the harm to the copyright holder outweighs any harm to the infringer. *Accusoft Corp.*, 923 F. Supp. at 295 (granting injunction). In this case, the defendants will suffer absolutely no harm if required to cease all dissemination of the Bypass Code. In contrast, Microsystems -- as well as the public -- will continue to suffer irreparable harm unless the defendants are prohibited from distributing the Bypass Code.

II. Expedited Discovery and a Document Preservation Order Is Necessary to Determine the Extent of Microsystems' Irreparable Harm and To Promote Mitigation of Damages  
Expedited discovery is appropriately where, as here, delay may result in continued irreparable harm. See, e.g., *Express One Int'l, Inc. v. U.S. Postal Service*, 814 F. Supp. 87, 92 (D.D.C. 1992) (enjoining contract and granting expedited discovery); *Polo Fashions, Inc. v Everything Goes*, No. 84-11549-K, slip op. at 7-9 (D. Mass. May 18, 1984) (granting expedited discovery and temporary restraining order ex parte "because it is the only method of preserving a state of affairs in which the Court can provide effective final relief"). Expedited discovery is also appropriate to "enable the court to judge the parties' interests and respective

chances for success on the merits." *Edudata Corp. v. Scientific Computers, Inc.*, 599 F. Supp. 1084, 1088 (D. Minn.) (granting expedited discovery), *aff'd in part and rev'd in part* on other grounds, 746 F.2d 429 (8th Cir. 1984).

Microsystems is suffering irreparable harm from the publication of the Bypass Code on Jansson's and Skala's Web sites, but the full extent of the irreparable harm is presently unknown. Indeed, Microsystems needs to discover who has downloaded the Bypass Code to ensure that it is not distributed in further violation of Microsystems' copyrights. In addition, Microsystems needs further identification of Jansson and Skala for proper service of these papers and the Verified Complaint. In short, given the speed with which information spreads on the Internet, Microsystems is entitled to know more about Jansson and Skala and the breadth of the impact of their posting without waiting for the traditional discovery mileposts.

Microsystems' requested discovery is narrowly tailored and asks Scandinavia Online and Islandnet only to respond to two document requests to provide information easily accessible to them and the usual time provided by the Rules is unnecessary.

Microsystems also requests that this Court issue a document preservation order which would require all defendants to preserve and hold inviolate Web sites, documents, source code and binaries relating to Cyber Patrol and the Web sites discussed above.

## CONCLUSION

For the foregoing reasons, Microsystems respectfully requests that the Court enter a temporary restraining order against the defendants and grant the requested expedited discovery and document preservation order.

Dated: March 15, 2000

Respectfully submitted,

---

Irwin B. Schwartz BBO#548763  
Joel G. Beckman BBO#553086

Laura N. Kling BBO#638313  
SCHWARTZ and NYSTROM, LLC  
419 Boylston Street  
Boston, Massachusetts 02116  
(617) 421-1800  
(617) 421-1810 (fax)

Counsel for Microsystems  
Software, Corp. and Mattel, Inc.

As the Ninth Circuit has explained, reverse engineering is a prima facie violation of copyright laws and is only permitted under narrow fair use exceptions inapplicable here. Sony Computer Entertainment, Inc. v. Connectix Corp., --- F.3d ---, 53 U.S.P.Q.2d 1705, 2000 WL 144399 \*6 (9th Cir. 2000); Sega Enter. LTD. v. Accolade, Inc., 977 F.2d 1510, 1518 (9th Cir. 1993) (holding that disassembly of copyrighted object code is, as a matter of law, a fair use only under narrow exceptions).

The facts are taken from the Verified Complaint, cited as (Ver. Comp. ).

A copy of the press release is attached to the Verified Complaint as Exhibit A. The Web address is redacted to prevent further harm, but will be provided in camera.

In enacting 47 U.S.C. § 231, The Child Online Protection Act, Congress stated its intent as follows:

The Congress finds that . . . while custody, care and nurture of the child resides first with the parent, the widespread availability of the Internet presents opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental control; . . . The protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them is a compelling governmental interest; . . . notwithstanding the existence of protections that limit the distribution over the World Wide Web of material that is harmful to minors, parents, educators, and industry must continue efforts to find ways to protect children from being exposed to harmful material found on the Internet

Pub. L. 105-277, Div. C. Title XIV, § 1402 (October 12, 1998).