

No. 00-1503

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

Microsystems Software, Inc.,

Plaintiff-Appellee,

v.

Scandinavia Online AB, Islandnet.com,
Eddy L.O. Jansson, and Matthew Skala,

Defendants-Appellees

Waldo Jaquith, Lindsay Haisley, Bennett Haselton

Appellants

On Appeal From The United States District Court
For The District of Massachusetts

**BRIEF OF AMICI CURIAE
IN SUPPORT OF REVERSAL**

Charles R. Nesson
Lawrence Lessig
Jonathan L. Zittrain
Diane Cabell
1563 Massachusetts Avenue
Cambridge, MA 02138
(617) 495-7547

and

Association for Computing
Machinery Committee on
Law and Computing Technology
by: Andrew Grosso
(First Circuit Bar #21840)
2121 K Street, NW Ste. 800
Washington, D.C. 20037

STATEMENT OF INTEREST

Charles R. Nesson is the William F. Weld Professor of Law and Director of the Berkman Center for Internet & Society at Harvard Law School. Lawrence Lessig is the Berkman Professor of Entrepreneurial Legal Studies at Harvard Law School. Jonathan Zittrain is the Executive Director of the Berkman Center. Diane Cabell is a Berkman fellow in Intellectual Property studies and is a practitioner in that field of law. Professor Nesson has directed the Berkman Center's research and activities studying Internet speech issues. Professor Lessig has authored many articles and essays relating to the regulation of access of children to material deemed harmful to minors. Professor Zittrain has lectured extensively on Internet free speech issues. These amici file this brief in their individual, not institutional, capacities.

Joining in this brief as well is the Association for Computing Machinery ("ACM")'s Committee on Law and Computing Technology ("ACM Law"). Founded in 1947, ACM is the world's first educational and scientific computing society. Today, ACM is an international scientific and educational organization dedicated to advancing the arts, sciences, and applications of information technology. With a world-wide membership of 80,000,

ACM functions as a locus for computing professionals and students working in the various fields of Information Technology. ACM has long advocated against censorship on the Internet. ACM studies, and expresses its opinion on, legal issues through ACM Law.

TABLE OF CONTENTS

STATEMENT OF INTEREST	i
TABLE OF CONTENTS.....	iii
AUTHORITIES.....	iv
SUMMARY OF ARGUMENT.....	1
ARGUMENT	
I. Courts should approach actions that threaten the free flow of ideas and information in cyberspace with caution.....	2
A. <i>Reno v. ACLU</i> sets the standard for evaluating regulations that affect the free flow of information in cyberspace	4
B. The principles of <i>Reno v. ACLU</i> apply equally forcefully in the copyright context as applied in cyberspace	6
C. These First Amendment principles counsel a Court to proceed with caution when applying novel copyright law to activities in cyberspace.	9
II. The expressive activities engaged in by Appellants are vital to the preservation of the free flow of ideas and information in cyberspace	11
A. The ultimate resolution of the question how best to protect kids from speech deemed “harmful to minors” has not yet been resolved.....	12
B. “Censorware” has been a highly controversial “solution” to the problem of protecting children in cyberspace	14
C. An active and vibrant debate about this matter of public import requires a special sensitivity by courts in enforcing legitimate copyright interests.....	16
CONCLUSION	20

AUTHORITIES

ERROR! NO TABLE OF AUTHORITIES ENTRIES
FOUND.ERROR! NO TABLE OF AUTHORITIES ENTRIES
FOUND.ERROR! NO TABLE OF AUTHORITIES ENTRIES
FOUND.

SUMMARY OF ARGUMENT

1. The district court improperly weighed the free speech interests implicated by plaintiff's actions, ignoring the method established by *Reno v. ACLU* for addressing free speech issues raised by the Internet. That method requires a court to weigh the effect of new or novel applications of law on speech in the Internet before applying that law to speech on the Internet. The court below instead summarily enjoined appellants without properly considering the interests at stake.

2. The free speech issues raised by this case are significant and unresolved. They implicate a general debate about how best to enable parental control over their children while on the Internet, without interfering with the free speech interests of other adults. The district court's injunction short circuits that debate, using the power of a federal injunction to disable effective critique of one solution to enabling parental control — plaintiff's products. This is an improper use of federal injunctive power.

ARGUMENT

The issues in this case reach far beyond a single piece of software, and the code written to defeat that software. Amici offer this brief to sketch how. The district court, while acknowledging that the case raised a “complex and

significant issue relating to copyright law,” did not fully acknowledge the implications of its decision for a very different debate: how to protect children from inappropriate speech on the Internet while simultaneously protecting free speech on the Internet. The Court’s decision is inconsistent with the Supreme Court’s instructions for treating cases that raise new applications of law implicating free speech interests on the Internet. We urge this Court to correct both the result in this case (by vacating the injunction granted) and to make clear the proper procedure for district courts in similar cases.

I. COURTS SHOULD APPROACH ACTIONS THAT THREATEN THE FREE FLOW OF IDEAS AND INFORMATION IN CYBERSPACE WITH CAUTION

The defendants in this case created software (“cpHack”) that, among other capabilities, makes it possible to identify the sites that plaintiff’s software (“CyberPatrol”) blocked. The appellants, and others, copied that software (with the permission of its authors) and made it available on the Internet. This publication made it possible for others to see the kinds of sites that CyberPatrol was blocking, and to evaluate whether the product was performing according to its promise.

CyberPatrol objected to this use of its software. It raced into court seeking a nationwide injunction stopping the distribution of cpHack. After a summary proceeding, the district court granted that injunction, without understanding the debate within which this software is a contestant, and ignoring the free speech costs of an injunction on an ongoing political argument. The Court thus used its power to interfere with a debate about a matter of fundamental import to the architecture of free speech in cyberspace.

The court's summary action was inconsistent with the approach that the Supreme Court has mandated for cases implicating free speech on the Internet. Where a new or novel application of federal law affects important free speech interests on the Net, federal courts should approach those questions with caution. They should hesitate before entering extraordinary relief, and should afford the affected parties an adequate opportunity to present the free speech issues at stake.

This is not because law does not apply to the Internet, or because behavior in "cyberspace" should be immune from ordinary regulation. There is no doubt that existing law, and the values that it represents — including the values embodied in copyright law — should apply to behavior in cyberspace

just as to real space. But striking the proper balance in cyberspace, and understanding the effect that law applied to cyberspace will have, will take time and a patient and conservative judicial attitude. Rather than racing to silence speech, courts must permit defendants, or those whose speech is restricted, an adequate opportunity to explain the effect of that regulation, and to explain the free speech interests at stake. That opportunity was denied appellants below.

A. *Reno v. ACLU* sets the standard for evaluating regulations that affect the free flow of information in cyberspace

The Supreme Court established this principle of deference in its first consideration of a law targeted directly at speech on the Internet — Congress’ 1996 Communications Decency Act. Telecommunications Act of 1996, Pub. L 104-104, Title V, 110 Stat. 56, 133-43 (“CDA”). That law purported to carry into cyberspace a fairly common restriction on access to certain adult speech — that minors be barred from accessing such material.

The statute’s objective, the Court acknowledged, was “compelling.” *Reno v. ACLU*, 521 U.S. 844, 869 (1997). State regulation advancing this objective, as the concurrence noted, was common. *Id.*, at 887 n.1 (O’Connor, J, concurring). Nonetheless, the Supreme Court approached this question

much more cautiously than it had approached the same question raised outside of the context of the Internet. See Lawrence Lessig, *What Things Regulate Speech*, 38 *Jurimetrics* 629 (Summer 1998) (comparing CDA to regulation of adult-vending machines). Recognizing the extraordinary importance of the Internet as a source for free speech and artistic creativity, the Court was careful to assure that this regulation would not overly burden or chill important free speech activity. Compare *United States v. Playboy Entertainment Group, Inc.*, 120 S. Ct. 1878 (2000) (similar approach applied to cable regulation).

The Court evinced this concern through a patient review of the effect that Congress' regulation would have on free speech activities, and a consideration of whether the restriction was necessary (in light of alternative measures) for achieving the same legislative end. *Id.*, 521 U.S., at 877-79. The Court concluded that Congress' ends extended beyond legitimate state interests, and that its means were more burdensome than necessary. It therefore invalidated the statute.

B. The principles of *Reno v. ACLU* apply equally forcefully in the copyright context as applied in cyberspace

The statute at issue in *Reno* was a law regulating “indecent” speech in cyberspace. Though recognizing the legitimacy of the interest at stake, 521 U.S., at 849 (“legitimacy and importance of the congressional goal of protecting children from harmful materials”), the Court was careful to examine the regulation’s effect on speech in cyberspace before ratifying that the law’s force.

The same approach, we submit, should apply to novel or broad applications of copyright law to speech in cyberspace. Here too, for the same reasons the Court offered in *Reno*, courts should weigh carefully the effect of such regulation on speech in cyberspace before they invoke the injunctive power of a federal court. Not *all* copyright cases: clear pirating behavior, for example, should be quickly and directly remedied. See, e.g., *Playboy Enterprises v. Sanfilippo*, 1998 U.S. Dist. LEXIS 5125, 46 U.S.P.Q.2D (BNA) 1350 (SD Cal 1998) (commercial adult web site sold access to thousands of unauthorized copies of Playboy’s images). But when copyright law is relied upon to restrict behavior that does not reach the core of copyright interests — when it applies, that is, to applications of copyright that are new or novel,

or without clear jurisdictional merit — then, following *Reno*, Courts should not resolve these questions in a summary fashion.

The instant case is an example of the point. The application of copyright law to foreign defendants, and those deemed acting “in concert” merely by mirroring defendant’s site, is a broad and novel application of copyright law. Br. App., at 30-31. We agree with appellants that United States copyright law does not reach this behavior. But whether it does or does not, it is not clear that it does. In such a case, where there is no clear copyright interest at stake, courts should hesitate before issuing nationwide injunctions silencing protected speech.

This conclusion follows directly from the principles of *Reno*. Like a law regulating “indecentcy,” copyright law regulates speech. Whether copyright law is, as some have argued, a content-based regulation of speech, see Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 Duke L.J. 147 (1998), or a content-neutral regulation of speech, see, e.g., *Dr. Seuss Enters. v. Penguin Books USA, Inc.*, 109 F.3d 1394, 1403 n.11 (9th Cir. 1997), it is a law by Congress that purports to restrict the ability of some to utter certain words, or words drawn

from other creative “writings.” 17 U.S.C. §106. Thus, even if considered just a content-neutral regulation of speech, copyright law must still advance an “important governmental interest,” without restricting more speech than “necessary” to advance that interest.” *Turner Broadcasting System, Inc. v. F.C.C.*, 520 U.S. 180, 189 (1997) (describing standard for intermediate scrutiny).

This is not to say that copyright law is inconsistent with the First Amendment. As the Supreme Court explained in *Harper & Row*, copyright law is fully consistent with the values of free speech. *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539 (1985). By functioning as an “engine of free expression,” *id.*, 558, stimulating authors to produce where they otherwise would have insufficient incentive to produce, copyright plainly does not “abridge” speech contrary to the requirements of the First Amendment. But as many have recognized, *Lee v. Runge*, 404 U.S. 887, 892 (1971) (Douglas, dissenting from denial of cert.), Melville B. Nimmer, *Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?*, 17 UCLA L. Rev. 1180 (1970), copyright is nonetheless constrained by important First Amendment values. These values check the scope of copyright law’s protections, limiting its reach in certain contexts.

These limits include at least the requirement of “fair use,” and the requirement that copyright protect expression only (not ideas). See, e.g., *Los Angeles News Service v. Tullo*, 973 F.2d 791, 795-96 (9th Cir. 1992) (“[c]opyright law incorporates First Amendment goals” by way of the idea-expression distinction and the fair use doctrine). They should also be understood to restrict the manner in which copyright claims might be pressed.

C. These First Amendment principles counsel a Court to proceed with caution when applying novel copyright law to activities in cyberspace.

Amici do not question the importance of protecting legitimate copyright interests in cyberspace. Nor do we doubt that courts should use their power to stop pirating or other illegal copyright behavior. But we do believe that in light of the attitude that the Court adopted in *Reno*, speech regulation through copyright must proceed cautiously. This Court must be convinced that the regulations effected through copyright do not reach beyond their legitimate ends when applied to activities in cyberspace, and that these regulations, though clearly legitimate, not restrict more speech than necessary to advance important governmental interests.

The district court did not properly entertain this inquiry. The urgency to enjoin appellants that the court expressed was not an urgency to protect plaintiff against the theft of their intellectual property. The urgency that the court relied upon was the urgency of protecting kids from speech from which their parents wanted them to be shielded. Stipulated Permanent Injunction, *Microsystems Software Inc. v. Scandinavia Online*, No. 00-10488, ¶ 53 (March 28, 2000) . That interest, however, was precisely the interest at stake in *Reno*. 521 U.S., at 849. If it was insufficient in *Reno* to displace the careful and balanced consideration that the lower and Supreme Court gave to the free speech interests at stake, so too should it be insufficient in this case.

Our claim is not that appellants deserve immunity from the copyright laws. Nor is it that cyberspace requires less vigorous or effective enforcement of copyright laws than real space does. Our argument is simply that until the contours of regulation in cyberspace are well understood, a court should grant the party whose speech in cyberspace is being regulated an adequate opportunity to demonstrate the harmful effects of that regulation on protected speech. Appellants did not have that opportunity here.

II. THE EXPRESSIVE ACTIVITIES ENGAGED IN BY APPELLANTS ARE VITAL TO THE PRESERVATION OF THE FREE FLOW OF IDEAS AND INFORMATION IN CYBERSPACE

The defendants in this case were not pirates. Their aim was not to copy plaintiff's product, and sell it to others. Neither was it their objective to obtain a product from plaintiff that they have not paid for. Everyone who uses the software at issue in this case necessarily does so with plaintiff's product. Defendant's conduct did not enable anyone to get that product without paying the appropriate price.

Instead, the behavior attacked in this action is (1) the reverse engineering of plaintiff's product, for the purposes of (a) understanding how it functions, (b) revealing the kinds of sites the product blocks, and (c) disabling the product, and (2) the mirroring or linking to sites with the reverse engineered code. The questions thus raised are (1) whether reverse engineering by foreign defendants in foreign countries violates either copyright law, or the license under which CyberPatrol was issued, and (2) whether merely linking or mirroring the product of such reverse engineering constitutes acting "in concert" with the defendants.

Amici agree with appellants that copyright law neither applies to the defendants in this case, nor should be read to proscribe the mirroring behavior engaged in by appellants. Br. Apps. 29-34. Our aim in this brief, however, is to place this technical jurisdictional issue in context. It is critical that this Court view this issue against the background of the debate within which it arises.

A. The ultimate resolution of the question how best to protect kids from speech deemed “harmful to minors” has not yet been resolved.

CyberPatrol is one of many products that have been developed to help parents block material they deem inappropriate for their children from their children. The range and diversity of these products is wide, and the techniques used differ. Some build “white lists” of sites that are appropriate for children.¹ Others build “black lists” of sites that are inappropriate for children. See *Reno*, 521 U.S., at 890 (O’Connor, J., concurring) (describing Cyber Patrol). Others offer a mix of these two strategies.² As a class, these

¹ This, for example, is the technique promoted by Apple Computer Company. See <http://itools.mac.com/KidSafe_home.html>

² See the resources at <http://www.epic.org/free_speech/censorware/>. For an examination of the specific problems with popular content blocking software, see <<http://www.peacefire.org/censorware/>>.

technologies represent an innovative way to deal with a problem deemed important by many parents and government officials.

These technologies, however, grow out of a bigger debate: namely, what mix of techniques for zoning children from inappropriate speech is most protective of free speech interests generally. Some have advocated law as the means to effect that zoning; others have promoted software as the means to effect that zoning; and others still have invoked simple norms of decency to induce providers to take steps to separate children from inappropriate material. See *Pornography: Free Speech or Censorship in Cyberspace*, 3 B.U. J. Sci. & Tech. L. 3 (1997). These are three very different methods for dealing with the same problem. Which one technique, or mix of techniques, is best is still unknown, and highly controversial.

Congress's first effort at protecting children was through law. The CDA was an attempt by Congress to mandate barriers between children and "indecent" speech. When the Supreme Court invalidated that regulation, the Court mentioned other technologies that might well supply the needed zoning without regulation. See *Reno*, 521 U.S., at 877; *id.*, at 890 (O'Connor, J.,

concurring). *Reno* thus created a strong incentive for the market to develop such programs. CyberPatrol was a beneficiary of this decision.

But the Supreme Court in *Reno* neither determined that private blocking software would be effective, nor suggested that private blocking software would not raise other free speech concerns. Indeed, the Court was quite tentative in its conclusions about what technology, or mix of technology and law, might best effect the protection parents want consistent with the values of free speech that the Internet supported. 521 U.S., at 877-79. In no way did the Court indicate that this debate had been resolved, nor did it endorse any one solution over another.

B. “Censorware” has been a highly controversial “solution” to the problem of protecting children in cyberspace

Since *Reno*, technologies that block access (called by their opponents, “censorware”) have come under increasing attack. See, e.g., *supra* note 2. These attacks are not by people who want children to get access to “pornographic speech.” Instead, these attacks have grown from increasing awareness that the scope of speech blocked by these technologies is often much wider than the products advertise.

This realization has led many to question the value of “censorware” as a solution to the problem of zoning children from material deemed “harmful to minors.” See, e.g., Hiawatha Bray, *A Faulty Censor*, Boston Globe, Dec. 30, 1999, at D1; Amy Harmon, *Ideological Foes Meet on Web Decency*, N.T. Times, Dec. 1, 1997, at D1; Seth Schiesel, *How Web Smut is Regulated May Depend on Tools to Filter It*, N.Y. Times, Mar. 24, 1997, at D5. If the technology effectively erases from the Internet important and valuable speech — beyond that speech the government has an interest in blocking — then many have come to believe that other solutions might be better.

Appellants’ counsel in this case, the ACLU, is a perfect example of this trend. While the ACLU led the challenge against the CDA, and while counsel arguing that case before the Supreme Court pointed to private blocking software as an alternative to regulation,³ the ACLU has been quick to criticize blocking software in light of what it has come to learn about how such software effects free speech in cyberspace. See *Fahrenheit451.2: Is Cyberspace Burning?*, <<http://www.aclu.org/issues/cyber/bu-rning.html>>.

³ Oral Argument of Bruce J. Ennis on Behalf of Appellees. See <<http://www.aclu.org/issues/cyber/trial/sctran.html#ennis>> (“The court below found as a fact, at pages 32a to 42a of the appendix to the jurisdictional statement, that there is a broad range of technologies and software programs that enable parents either completely to block all access to the Inter-

Such shifts are not surprising. No one yet has a good understanding of how different techniques for zoning speech in cyberspace will actually work. It is therefore unremarkable that a technique thought a solution initially, upon reflection, turns out to have unintended consequences. Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 Mich. L. Rev. 395, 422-26 (1999) (discussing unintended consequences). What is crucial in a context of such uncertainty is to preserve the opportunity for these different technologies to be understood and criticized, and to ensure that opponents of these technologies have the opportunity to investigate and criticize what these technologies do.

C. An active and vibrant debate about this matter of public import requires a special sensitivity by courts in enforcing legitimate copyright interests.

In the context of such a controversy, it is important that Courts not become a tool to short circuit a political debate. For the essence of plaintiff's actions is to make it more difficult for consumers and those interested in this more general free speech debate to understand what kind of speech is

net, if the parents are really concerned or, more selectively, to screen and filter access to the Internet if they want to allow their children to have access to certain parts of the Internet but not to others”).

blocked by censorware generally. Plaintiff is trying to use the law of copyright to silence criticism of its product.

Plaintiff has done this first by asserting, contrary to strong legal authority, *see, e.g., Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596, 603 (9th Cir. 2000), that the mere act of reverse engineering CyberPatrol violates copyright law. This claim would be weak at best if made against a defendant engaging in this behavior within the United States; it is paper-thin when made against foreign citizens for behavior engaged in by them in their own country. *Twin Books Corp. v. Walt Disney Co.*, 83 F.3d 1162, 1166-67 (9th Cir. 1996) (rejecting extra-territorial application of copyright law). Nonetheless, the threat of litigation, and the costs that it imposes on ordinary citizens, was enough, in this case, to force the defendants quickly to settle the case. The mere threat of litigation was enough to silence this critical speech.

Plaintiff persuaded the lower Court that it was entitled to prevent reverse engineering of CyberPatrol because it distributes the program subject to a license that forbids reverse engineering. The inappropriateness of this use of law—primarily contract law, in the form of a license — is apparent

outside the context of cyberspace. First, there was not even a showing that defendants received CyberPatrol subject to a license. As Judge Easterbrook noted in *ProCD v. Zeidenberg*, 86 F.3d 1447, 1454 (7th Cir. 1996), a license only binds parties to the license. “[S]trangers may do as they please.” *Id.*

But second, and more fundamentally, to invoke the equitable power of a federal court to enforce such a license is contrary to any legitimate public policy interest. Imagine that the maker of the Corvair had tried to use a license to stop Ralph Nader from disassembling and testing the Corvair, to determine its safety. Ralph Nader, *Unsafe At Any Speed; The Designed-In Dangers Of The American Automobile* (1965). Or imagine a license prohibiting the use of software by anyone whose purpose is to evaluate the software against security attacks. In these cases, it would be clear that the law was being used as a tool to silence important speech critical of a product, or more generally, about that product’s effect on other important public values.

This, we submit, is precisely the issue raised by this case. Plaintiff tries to hide behind copyright and contract law to keep secret its list of internet “banned books,” both to protect itself from the embarrassment of mistaken classification, and to protect itself from the effect that such speech

might have on its product generally. It is not protecting that list from a competitor; it is hiding it from its customers. It is afraid, in other words, that if people understood the limitations of its software, or the effect its software might have upon free speech generally, then customers would be less likely to buy its software. It thus uses copyright law to mislead the public into buying a product which they may not buy if they knew more about the product.

This is an inappropriate use of copyright law. The objective of copyright law is to restrict pirating, so as to give copyright holders a sufficient incentive to produce. The law has no interest in silencing criticism of those products, or in facilitating non-transparent censorship in a medium such as the Internet.

In light of the important free speech issues at stake in this case, plaintiff has not succeeded in demonstrating the equity in extraordinary relief. The essence of defendants' behavior, and likewise the behavior of appellants, is to facilitate criticism of plaintiff's product. The law of copyright has no interest in stifling criticism. See *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 591-92 (1994). Plaintiff has not demonstrated any substantial harm

beyond this criticism. It has failed to meet the high standard for invoking a federal court's injunctive power.

CONCLUSION

For the foregoing reasons, this Court should vacate the injunction granted below.

Respectfully submitted,

Charles R. Nesson,
Lawrence Lessig,
Jonathan Zittrain, and
Diane Cabell
1563 Massachusetts Avenue,
Cambridge, Massachusetts 02138
617-495-7547

and

Association for Computing
Machinery Committee on
Law and Computing Technology
by: Andrew Grosso
(First Circuit Bar #21840)
2121 K Street, NW Ste. 800
Washington, D.C. 20037
202-835-2682

Dated: June 13, 2000