No. 04-480

In The Supreme Court of the United States

METRO-GOLDWYN-MAYER STUDIOS, INC., *et al.*,

Petitioners,

v.

GROKSTER, LTD., *et al.*,

Respondents.

On Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

BRIEF *AMICI CURIAE* OF COMPUTER SCIENCE PROFESSORS HAROLD ABELSON, THOMAS ANDERSON, ANDREW W. APPEL, STEVEN M. BELLOVIN, DAN BONEH, DAVID CLARK, DAVID J. FARBER, JOAN FEIGENBAUM, EDWARD W. FELTEN, ROBERT HARPER, M. FRANS KAASHOEK, BRIAN KERNIGHAN, JENNIFER REXFORD, JOHN C. REYNOLDS, AVIEL D. RUBIN, EUGENE H. SPAFFORD AND DAVID S. TOURETZKY SUGGESTING AFFIRMANCE OF THE JUDGMENT

VICTORIA K. HALL
LAW OFFICE OF
VICTORIA K. HALL
401 N. Washington St.
Suite 550
Rockville MD 20850
(301) 738-7677

JAMES S. TYRE*
LAW OFFICES OF
JAMES S. TYRE
10736 Jefferson Blvd., #512
Culver City, CA 90230
(310) 839-4114

**Counsel of Record*

Counsel for Amici Curiae

February 28, 2005

COCKLE LAW BRIEF PRINTING CO. (800) 225-6964
OR CALL COLLECT (402) 342-2831

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

MISCELLANEOUS

TABLE OF AUTHORITIES – Continued

Page

BRIEF *AMICI CURIAE* OF COMPUTER SCIENCE PROFESSORS SUGGESTING AFFIRMANCE OF THE JUDGMENT

These computer science professors, as *amici curiae*, respectfully submit that the judgment below should be affirmed.[1]

INTERESTS OF *AMICI CURIAE*

As more fully described in the Appendix, *amici* are 17 computer science professors at nine major universities in the United States.[2] Each *amicus* respects the value of intellectual property. All have published copyrighted works, some hold patents, and some have seen their copyrighted works made available without authorization on a peer-to-peer (P2P) file-sharing network. None condone the unlawful use of file-sharing technology. *Amici* submit this brief because *amici* are gravely concerned that the ability to deploy or improve new technologies that can be used for lawful and unlawful purposes will be severely constrained if the Court scales back the protections inherent in the

[1] Per Rule 37.6, *amici* state that no counsel for any party has participated, in whole or in part, in writing this brief. The Distributed Computing Industry Association is defraying the out-of-pocket cost of printing this brief, but no person or entity other than *amici* or their counsel has made any other monetary contribution for preparing or submitting this brief. Counsel of record for *amici* is a Policy Fellow and an Advisory Board member of the Electronic Frontier Foundation, which is co-counsel for Respondent StreamCast Networks, Inc. Both titles are unpaid and honorary designations, for work unrelated to this case. The parties have consented to the filing of this brief.

[2] Affiliations are listed only to identify the *amici*, whose views expressed herein do not necessarily coincide with those of their respective institutions.

"capable of substantial noninfringing uses" test of *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984) (*Sony-Betamax*).

Amici are technology innovators who have been involved in major advances in Internet technology. David Clark was one of the original designers of the Internet, served as Chief Protocol Architect for the Internet in the 1980s, and has articulated the key design principles of the Internet such as the end-to-end arguments, *see* Section III, *infra*. Dr. Clark and his group created the first implementation of TCP/IP for the personal computer.[3] Steven Bellovin was one of the inventors of Usenet, an early and highly decentralized network. David Farber was responsible for the development of the first distributed computer system, was a principal in several major networking efforts, and was the co-principal of the pioneering NSF/DARPA-funded Gigabit Network Testbed Initiative. Eugene Spafford developed the first generally available intrusion detection system, and the first system security scanner. He also was the first person to develop software forensics techniques for cybercrime investigation. Other *amici* have made and are making equally important contributions to Internet technology.

Although some *amici*'s technology can be, has been and will be used for unlawful purposes as well as for lawful ones, *amici* have never before believed that their work would be threatened by others' unlawful use of their technology. For 21 years, the "capable of substantial noninfringing uses" test has protected those who developed new

[3] TCP/IP (Transmission Control Protocol/Internet Protocol) is the communication language that all computers use on the Internet.

technology capable of infringing and non-infringing uses – technology that benefits all. While technology innovators can guess at how a new technology will be used, only after its release will they truly know its uses, either as deployed initially or as modified.[4] The fact is that *Sony-Betamax* has been at the core of new technology development, because technologists deliberately design for multiple uses, and often cannot predict exactly what uses will be made of the technology.

A year ago, this Court recognized the need to " . . . safeguard the incentive to innovate . . . ."[5] *Sony-Betamax*'s protection provides such an incentive, in academia as well as in the private sector. If this Court should announce a more restrictive rule, those who create the latest advances in technology will halt or significantly scale back their work, for fear of massive copyright infringement damages. Such a rule will hinder technological progress, particularly involving computers and the Internet. Almost all new technology, whether coming from the private sector or from academia, builds on that which has come before. The best improvements, the best ideas, often derive from seeing how a technology performs in actual use, not solely

[4] *Amici* need look no further than Sony's own Betamax machines. They could record and play tapes of only one hour length, making difficult "librarying" of longer programs and other uses that the studios complained of at the time. *See Sony-Betamax*, 464 U.S. at 423. Other companies developed the competing VHS standard, which allowed playing and recording of longer tapes, and over time, that standard drove the Betamax out of the market. It also allowed the videotape rental and sale business to flourish, much to the benefit of the movie studios' profits.

[5] *Verizon Communications, Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 407 (2004) (for at least a limited time, innovators can rely on monopoly power).

in a laboratory test bed. But if Petitioners have their way, the ability to deploy or improve new technologies that can be used for both lawful and unlawful purposes will be constrained severely. This concern prompts *amici* to submit this brief.[6]

SUMMARY OF ARGUMENT

Amici write to call to the Court's attention several computer science issues raised by Petitioners and *amici* who filed concurrent with Petitioners, and to correct certain of their technical assertions. First, the United States' description of the Internet's design is wrong. P2P networks are not new developments in network design, but rather the design on which the Internet itself is based. Second, a P2P network design, where the work is done by the end user's machine, is preferable to a design which forces work (such as filtering) to be done within the network, because a P2P design can be robust and efficient. Third, because of the difficulty in designing distributed networks, advances in P2P network design – including BitTorrent and Respondents' software[7] – are crucial to developing the next generation of P2P networks, such as

[6] Petitioners argue that the Court of Appeals misapplied the rule of *Sony-Betamax*, rather than that the rule itself should be revisited. However, *amici* apprehend no way to reconcile Petitioners' arguments with the "capable of substantial noninfringing uses" test of *Sony-Betamax*.

[7] *Amici* are aware that Grokster and the FastTrack protocol it uses differ in many respects from Morpheus and the Gnutella protocol it uses. Indeed those differences have value to academicians and technologists. However, for the purpose of this brief, *amici* need not differentiate between the two.

the NSF-funded IRIS Project. Fourth, Petitioners' assertion that filtering software will work fails to consider that users cannot be forced to install the filter, filtering software is unproven or that users will find other ways to defeat the filter. Finally, while Petitioners state that infringers' anonymity makes legal action difficult, the truth is that Petitioners can obtain IP addresses easily and have filed lawsuits against more than 8,400 alleged infringers. Because Petitioners seek a remedy that will hobble advances in technology, while they have other means to obtain relief for infringement, *amici* ask the Court to affirm the judgment below.

ARGUMENT

I. NATURE OF THE INTERNET.

First, *amici* address statements in the United States' brief, *see* United States Br. at 2-3, that P2P design and file sharing are recent aberrations. To the contrary, they have been features of the Internet from its inception.[8] Thus, any liability rule applied to these technologies in general applies in general to the Internet also.

A network system uses P2P design if it allows any participant to act as a client, by requesting service from another participant, and to act as a server, by providing service in response to a client's request. Any network that treats its members as equals must use a P2P design.

[8] *See* Barry M. Leiner et al., *A Brief History of the Internet*, *at* http://www.isoc.org/internet/history/brief.shtml (last revised Dec. 10, 2003).

The very first Internet standards document,[9] dated April 7, 1969 and known as RFC 1, discusses the use of the nascent network to connect any user to any remote computer in what is now called a P2P fashion, and to transmit files between computers via these connections. Indeed, these are the only specific network building blocks (called "primitives") discussed in RFC 1.[10] Development of P2P interaction and file transfer has continued as the Internet has grown. Accordingly, any rules that might be applied to P2P technologies in general, or to file sharing systems in general, necessarily would apply to the Internet in general.

II. THE END-TO-END PRINCIPLE.

Second, *amici* address assertions that checking for infringement should be built into network design. On the contrary, certain functionality (such as using filters) should not be done at the network level. To order network designers to add functionality to the network to avoid liability is to force significant inefficiency into network design. Because leaving out such functionality may represent good engineering design, no negative inference regarding intent should be drawn if a designer chooses not to add this functionality.

One of the most important principles of network design, and one that underlies the Internet's design, is the end-to-end principle, which first appeared in a paper co-authored

---

[9] Steve Crocker, *Request for Comments 1: Host Software*, *at* http://www.faqs.org/ftp/rfc/rfc1.txt (Apr. 7, 1969).

[10] *Id.* at 6.

by one of these *amici*, David Clark.[11] The principle says that most functions should be provided at the endpoints of a network, rather than in the network itself. Because only the endpoints know precisely what they want from the network, the network cannot provide many functions correctly and efficiently. Examples, using email and teleconferencing, help explain the principle and why adding functionality in networks poses problems.

Suppose we want to transmit an email message from Alice to Bob, and we want to detect and correct any errors that might creep into the message's text between the time Alice writes it and the time Bob reads it. Such errors could creep in at several points: on Alice's computer while the message is waiting to be transmitted, on the network in transit from Alice's computer to Bob's computer, or while on Bob's computer before he reads it. The best way to provide appropriate error correction is to use an end-to-end mechanism. If errors must be detected and corrected, then a checksum[12] can be used. Alice's email program, at one endpoint, adds a checksum to the message as soon as she finishes writing it, and Bob's email program, at the other endpoint, verifies right before Bob reads the message that the text is consistent with the checksum. If errors are detected, Alice can retransmit the message.

---

[11] J.H. Saltzer et al., *End-to-End Arguments in System Design*, 2 ACM Transactions on Computer Sys. 277-88 (Nov. 1984), *available at* http://mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf.

[12] A checksum is a value computed from the content of a message that can be used as a "signature" to verify its accuracy. Virtually any change in a message's length or content will alter the checksum, allowing transmission errors to be readily detected.

If Alice and Bob want end-to-end protection, they need to use an end-to-end mechanism as described above. Once they do this, it would be redundant to add an error-correction mechanism into the network itself. Worse yet, adding error detection and correction would make the network both more expensive, and less flexible for other uses.

For example, in some applications, such as teleconferencing, it is better to accept minor errors than to try to fix them. A little snow on the screen is better than having the image freeze entirely while the system tries to retransmit the damaged image. A network that tried to fix errors would be much worse for teleconferencing than one that did not. Thus, adding functionality to a network can make the network both more expensive and less useful.

Networks that are designed according to the end-to-end principle are general-purpose, meaning that they can be extended for a wide range of uses that were not anticipated at the time of their design. General-purpose networks derive their generality from the fact that they do not try to understand the information that is flowing through them. The telephone network, a familiar example of a general-purpose network, is designed to carry any voice (or voice-like audio signal) from Point A to Point B, without trying to understand the meaning of the sound or the content of the conversation, if indeed it is a conversation. Designing a network this way makes the network easier to build. After all, it is much easier to transmit raw voice sounds than to understand the content of speech.

But perhaps more important, because the telephone network was designed to carry raw sounds, it could be adapted later to a wide range of uses unforeseen by its

designers. Alexander Graham Bell probably did not foresee faxes, answering machines, or voice mail. He could not have predicted that some day vending machines would make telephone calls when they ran out of candy bars. He did not need to foresee these developments, because he designed a general-purpose network that could support whatever later uses that were found.

The Internet is the ultimate general-purpose network. With its end-to-end design, the Internet serves a much broader purpose than the telephone network, being able to carry any type of digitized content, rather than only audio signals. The general-purpose nature of the Internet is the reason for its rapid evolution and its adoption by broad segments of our society and economy.

In light of the astonishing usefulness of general-purpose networks such as the telephone network and the Internet, a designer's decision not to include some function in the network should not, in itself, be seen as evidence of any particular intent. *Amici* have no knowledge of the particular motives of Respondents, but caution against the inference that a particular design decision, such as a decision to include encryption or not to use filtering technologies, necessarily represents bad faith. It may simply represent good, conservative engineering. Here, the United States seems to agree:

> To the extent that petitioners' argument concerning vicarious liability could be construed as suggesting the imposition of [] an obligation [on Respondents to control their customers' infringing conduct], such a rule is neither desirable nor supported by precedent. [. . .] The "right and ability to supervise" element of vicarious liability . . . has never, to our knowledge, been held to be

> satisfied by the mere fact that the defendant *could* restructure its relations or its product to obtain such an ability. [. . .] The imposition of an independent obligation to arrange one's product or relations in a way to permit the seller to retain control would have the undesirable effect of chilling technological innovation and constraining the product development options of developers of software and other digital technologies.

United States Br. at 19 n.3 (citations and quotes omitted).

III. THE DIFFICULTY OF DESIGNING DISTRIBUTED NETWORKS.

Third, designing large-scale network systems poses formidable challenges. To create the next generation of networks, research scientists and software developers constantly seek new and better network designs and software. Due to the challenges in network design, and numerous research questions in this area, *amici* respectfully urge the Court to be very cautious in addressing liability rules so that such rules do not dictate the design of such software, or order the redesign of systems that function efficiently already.

Designing large-scale network systems is notoriously difficult. Large networks must cope with vexing issues of scale, reliability, robustness and security that simply do not arise in smaller networks. Consequently, researchers are looking more to P2P networks, which offer significant advantages over client-server networks that have bottlenecking problems when many users try to access a web site, and can be easily taken down due to single points of failure and denial of service attacks. When someone builds successfully a large network, they teach valuable lessons

about the design of such networks. The networks created by the users of Respondents' software have certainly taught such lessons, as have other P2P systems, which designers use to advance research and product development.

One beneficiary of such lessons is the National Science Foundation-funded Infrastructure for Resilient Internet Systems (IRIS) project.[13] IRIS, co-led by one of these *amici*, Frans Kaashoek, is a multi-institution collaboration, centered at MIT and U.C. Berkeley and funded by a $12 million NSF grant.[14] IRIS seeks to use a P2P design strategy to support large-scale Internet services in a manner more scalable, reliable, and secure than is currently possible. Without Respondents' success in developing software that allows end users to participate in a large scale P2P network, scientists on the IRIS Project would have more difficulty in their research. Petitioners' lawsuits against designers such as Respondents whose software allows users to create a network threaten research necessary to build better networks.

However, the chilling effect of lawsuits – actual or threatened – is perhaps better illustrated by reference to BitTorrent. Unlike IRIS, BitTorrent is a type of P2P network software that is in widespread use already. Developed by Bram Cohen, BitTorrent is an important advance in large scale network technology because of its

---

[13] IRIS: Infrastructure for Resilient Internet Systems, *at* http://www.project-iris.net (last visited Feb. 6, 2005)

[14] David Cohen, *New P2P Network Funded by U.S. Government*, New Scientist, Oct. 1, 2002, *at* http://www.newscientist.com/article.ns?id=dn2861.

usefulness in copying large files.[15] BitTorrent allows a large number of computers that have a file to share in copying it to a person seeking it. Because the sharing is simultaneous (each computer that has the file transfers a portion of it at the same time as other computers that have it) the transfer can avoid or lessen bottlenecking that occurs if the entire file is copied from a single computer. Further, as soon as the person has a portion of the file, her computer shares in making it available to others who seek it. In BitTorrent parlance, this is called swarming.

BitTorrent itself does not support file searching. Consequently, a common way of determining whether a file has been torrented (formatted so that it can be copied using BitTorrent) is to look at a so-called tracker site: a site that keeps track of torrented files, and allows one to join in the swarm if one wants to copy a file. For example, Red Hat, a major packager of Linux software, uses a torrent tracker to save bandwidth in the distribution of its software.[16] As another example, Peter Jackson, the Producer of the Lord of the Rings movie trilogy, now is producing a remake of King Kong. Jackson is keeping an online production diary of the making of the film, that includes both text and video. The video files being large, he is using BitTorrent to share the work of distributing the files.[17] As still another, after the Tsunami, naturally there was great

[15] Like any design, BitTorrent has strengths and weaknesses, and *amici* can learn from both.

[16] Duke University maintains the tracker for Red Hat's Fedora Core Linux software, Bittorrent for torrent.linux.duke.edu, *at* http://torrent.linux.duke.edu (last visited Feb. 18, 2005).

[17] Kong is King.net | King Kong | Peter Jackson's Production Diary, *at* http://www.kongisking.net/kong2005/proddiary (last visited Feb. 24, 2005).

interest in seeing the videos that had been taken on scene. A number of trackers are available for those amateur videos.[18]

In December 2004, the movie studios commenced a series of legal actions against certain tracker sites – sites that included tracks of the studios' copyrighted works. At the time, the studios seemed to appreciate the difference between the technology and its developer on the one hand, and unlawful uses of the technology on the other.[19] The MPAA anti-piracy chief acknowledged the existence of legal torrent sites.[20] However, by mid-February 2005, the MPAA apparently had changed its thinking:

> The industry is hoping that in a case scheduled for next month, the U.S. Supreme Court will rule against firms that produce file-sharing software, such as Morpheus and Grokster. Neither Cohen nor BitTorrent is named in the lawsuit, although an MPAA spokesman says Cohen is under scrutiny for continuing to develop the software "and making it easy to steal copyright material."[21]

Clearly, BitTorrent not only is capable of substantial noninfringing use, but in fact is used every day for substantial non-infringing purposes. A rule that would make a developer like Cohen secondarily liable for copyright

---

[18] *See, e.g.*, PunditGuy: Tsunami Videos, *at* http://www.punditguy.com/2004/12/horror.html (last visited Feb. 24, 2005).

[19] *See, e.g.*, Xeni Jardin, *Hollywood Wants BitTorrent Dead*, Wired News, Dec. 14, 2004, *at* http://www.wired.com/news/digiwood/0,1412,66034,00.html.

[20] *Id.*

[21] Daren Fonda, *Downloading Hollywood*, TIME, Feb. 14, 2005, *at* 43.

infringement, merely because his software can be and is used for infringing purposes would also cripple advances in large-scale network design. Such a rule surely would not safeguard the incentive to innovate.

IV. THE UNPROVEN EFFICACY OF CONTENT FILTERING TECHNOLOGIES.

Petitioners, and some *amici*[22] assert that Respondents should use various content filtering technologies, in an attempt to prevent infringement on the networks created by their users. Contrary to such assertions, the efficacy of these technologies is far from established. *Amici* wish to bring three things to the Court's attention.

First, the suggested filtering strategy would require filtering software to be installed on users' computers. Even assuming that Respondents have the right and ability to deliver such software to end users, there can be no way to ensure that software updates are installed, and stay installed. End users ultimately have control over which software is on their computers. If an end user does not want a software update, there is no way to make her take it. Indeed, a computer user who exercises proper security precautions should not allow any third party to install or upgrade software on her machine.

---

[22] United States Br. at 26; Am. Fed'n of Musicians of the U.S. & Can. et al. Br. at 19; Audible Magic Corp. et al. Br.; Bridgemar Servs. Ltd. Br.; Hollaar Br. at 20; Kids First Coalition et al. Br. at 8, 13; Macrovision Corp. Br. at 8, 11; Napster, LLC et al. Br. at 14; Nat'l Acad. of Recording Arts & Scis. et al. Br. at 18-21; Nat'l Ass'n of Recording Merchandisers Br. at 7 n.5, 19 n.21; Office of the Comm'r of Baseball et al. Br. at 14; Snocap, Inc. Br.; Utah et al. Br. at 20 & n.13, 24-26; Video Software Dealers Ass'n Br. at 16.

Second, it is important to recognize that the filtering technologies in question have not been subjected to any significant public testing or scrutiny. No demonstration has shown that these technologies would be effective in distinguishing infringing from noninfringing files if deployed in conjunction with software like Respondents'. No demonstration has shown that these technologies would scale to the extent necessary to be deployed successfully on large networks created by users of Respondents' software. While some *amici* who have filtering products they want to sell, have filed briefs in this case, some of their products are not even available for sale yet, let alone been subject to testing. Filter sellers, understandably, have high hopes for their products. These hopes should not be mistaken for evidence.

Third, experience shows that users respond to filtering and blocking technologies by devising methods to defeat the filter. For example, the Chinese government runs a filter, known colloquially as the "Great Firewall of China," that tries to restrict access from within China to certain Internet material of which the Chinese government disapproves – possibly including, at times, this Court's web site.[23] Chinese citizens, with the help of outsiders, have found many ways to defeat this firewall to read the forbidden material.

To predict the effect of filtering technologies, a static analysis, which assumes deployment of the technologies but ignores the likely responses of noncompliant users, is

[23] Jonathan Zittrain & Ben Edelman, *Empirical Analysis of Internet Filtering in China*, *at* http://cyber.law.harvard.edu:8080/filtering/china (last visited Feb. 18, 2005).

not sufficient. Instead, an accurate prediction of filter software effectiveness must use a dynamic analysis, which considers users' responses.

If filters were introduced as suggested by Petitioners, and assuming – despite lack of evidence – that the filters were deployable and would work exactly as Petitioners hope, noncompliant users would still have several methods for defeating them. For example, a user could encrypt files, to hide their contents, before submitting the files to Respondents' software; other users, on receiving the files, would decrypt them to recover the original contents. Respondents' software (and any filter incorporated into it) would then see the files only in encrypted form, and so would be unable to distinguish infringing files from noninfringing files. Suitable encryption tools are widely available.

Filter designers might respond by trying to detect and block encrypted files. That task is more difficult than it sounds, and besides, noncompliant users could respond by manipulating the encrypted files to look like innocuous content, using standard information-hiding technology. Each move by the filter designers would elicit a counter-move from the noncompliant users.

Because users would respond to filtering technology advances, the introduction of such technologies would not solve the infringement problem but would kick off an open-ended arms race between the filter designers and noncompliant users. To enter this arms race would be to take on recurring costs (in money and lost technical flexibility), in exchange for benefits that are at best uncertain. Further, turning secondary liability on this inevitable dynamic would embroil the courts in a continuing process

of evaluating and choosing new technologies intended to respond to these countermeasures.

The *Napster* case illustrates these points. After *Napster I*,[24] the Court of Appeals remanded the case to the district court for further proceedings. The district court then ordered Napster to filter file names of copyrighted works noticed by plaintiffs. *A&M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091, 1096 (9th Cir. 2002) (*Napster II*). When users responded by making alterations in file names or the spelling of titles or artists' names, Napster was required to identify and filter those variations. *Id.* When that did not work to the satisfaction of the district court, Napster installed audio fingerprinting technology, technology which relies on the "fingerprint" of the copyrighted work, and thus is not dependent on the file name or spelling adjustments. *Id.* at 1097.

Napster succeeded in "prevent[ing] sharing of much of plaintiffs' noticed copyrighted works." *Id.* at 1096. However, that was not good enough. The district court demanded zero error tolerance for plaintiffs' properly noticed works. *Id.* at 1098. When Napster could not achieve perfection, the court ordered Napster to shut down, and the Court of Appeals affirmed. *Id.* at 1099.

Though Petitioners and *amici* cite often to *Napster I*, the near total absence of *Napster II* in their briefs shows a reluctance to acknowledge that the filter software they speak of is mostly "vaporware" – non-existent. Some *amici* offer technology similar to that which failed to achieve zero error tolerance in *Napster II*. Some make grand

[24] *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

claims, but none guarantee or offer proof that they can achieve anything close to the zero error tolerance required in *Napster II*.

V. ANONYMITY.

Petitioners and some *amici* assert incorrectly that users of P2P networks are anonymous and hence need not fear enforcement.[25] The truth is, Respondents' software does little to prevent its users from being identified. Generally, providing anonymous, reliable communications among strangers is a difficult task. No demonstration has shown that a practical file-sharing system can provide such anonymity.

Respondents' software transfers files directly from the users who have them to the users who request them. Because of this, anyone who downloads a file learns the IP address of the person who is providing that file.[26] Anyone can connect to these networks and download files, in order to learn the IP addresses of users who offer them. The IP addresses can be used later to identify those who provide copyrighted files.[27] Petitioners (or their agents) and other copyright owners have used this method to sue more than 8,400 users of various P2P networks for direct

[25] Pet. Motion Picture Studio & Recording Co. Br. at 3-4; Am. Soc'y of Composers, Authors & Publishers et al. Br. at 9-10; Defenders of Prop. Rights Br. at 4; Kids First Coalition et al. Br. at 17-19; Office of Comm'r of Baseball et al. Br. at 4, 8-9.

[26] An IP address is a numeric value that identifies a particular "location" on the Internet.

[27] A user's IP address may change from time to time, but the user's Internet Service Provider will keep records that can be used to determine who was using a particular IP Address at a particular time.

infringement.[28] Thus, arguments that anonymity is a barrier to enforcement are false. As stated recently by the Register of Copyrights, The Honorable Marybeth Peters:

> Technology, however, makes [detection of infringement] much more possible – an individual's activity on peer-to-peer networks can be monitored and logged by the same computers that make the reproduction and distribution possible. This gives copyright owners a possibility of enforcement that they did not have before.

Marybeth Peters, *Copyright Enters the Public Domain*, 51 J. Copyright Soc'y 701, 708 (2004).

CONCLUSION

Amici urge the Court not to be lured into abandoning the *Sony-Betamax* "capable of substantial noninfringing uses" test, which has protected advances in technology so well. Abandoning this test will chill future development of Internet technologies. Petitioners claim otherwise, but Petitioners seem not to fully appreciate how new technologies are developed. From a purely technical standpoint, Respondents' products are not so very different from mainstream Internet technologies. Attempts to regulate or redesign large-scale network systems carry larger risks, and offer benefits much less certain than Petitioners

[28] *See* John Borland, *RIAA files 754 new file-swapping suits*, C|net news.com, Dec. 16, 2004, *at* http://news.com.com/RIAA+files+754+new+file-swapping+suits/2110-1027_3-5494259.html (7,706 lawsuits filed); John Borland, *RIAA sues 717 file-swappers*, C|net news.com, Jan. 27, 2005, *at* http://news.com.com/RIAA+sues+717+file-swappers/2110-1027_3-5553517.html (717 more lawsuits).

would have the Court believe. *Amici* ask the Court to take care to protect the scientists and engineers who are developing tomorrow's technology. *Amici* ask the Court to preserve the *Sony-Betamax* "capable of substantial noninfringing uses" test.

Respectfully submitted,

VICTORIA K. HALL
LAW OFFICE OF
VICTORIA K. HALL
401 N. Washington St.
Suite 550
Rockville MD 20850
(301) 738-7677

JAMES S. TYRE*
LAW OFFICES OF
JAMES S. TYRE
10736 Jefferson Blvd., #512
Culver City, CA 90230
(310) 839-4114

**Counsel of Record*

Counsel for Amici Curiae

February 28, 2005

APPENDIX – BRIEF BIOGRAPHIES OF *AMICI CURIAE*

Harold (Hal) Abelson[29] is Class of 1922 Professor of Electrical Engineering and Computer Science at MIT and a Fellow of the Institute of Electrical and Electronics Engineers (IEEE). He is the winner of the 1995 Taylor L. Booth Education Award given by IEEE Computer Society, cited for his continued contributions to the teaching of introductory computer science. At MIT, Abelson is co-director of the MIT-Microsoft Research Alliance in Educational Technology and co-chair of the MIT Council on Educational Technology. Together with his colleague Gerald Sussman, Abelson developed MIT's introductory computer science subject, "Structure and Interpretation of Computer Programs," which has had a world-wide impact on university computer-science education. Dr. Abelson teaches a course in collaboration with Harvard Law School, which deals with technical and policy issues relating to the Internet, including copyright management, content control, and privacy.

Thomas Anderson[30] is Professor in the Department of Computer Science and Engineering at the University of Washington. His research concerns the principles underlying the construction of secure, reliable and efficient large scale networks and distributed systems. He serves as Chair of the Steering Committee of the Planetlab Consortium, an

---

[29] Hal Abelson, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, *at* http://www.swiss.ai.mit.edu/~hal/hal.html (last visited Feb. 6, 2005).

[30] Tom Anderson, Department of Computer Science and Engineering, University of Washington, *at* http://www.cs.washington.edu/homes/tom (last visited Feb. 6, 2005).

association of over one hundred universities and corporations devoted to developing the next generation of Internet technologies.[31] Planetlab operates a network of over five hundred machines, spread over five continents, that can be used by researchers to test and deploy new planetary scale applications. An author of over 70 research papers, Anderson has won the National Science Foundation (NSF) Presidential Faculty Fellowship and the Sloan Research Fellowship.

Andrew W. Appel[32] is a Professor of Computer Science at Princeton University. He does research in computer security, virus prevention, programming languages, and compilers. He is a Fellow of the Association for Computing Machinery (ACM) and served for several years as Editor in Chief of ACM Transactions on Programming Languages and Systems. Dr. Appel served as a primary technical expert for nine non-settling States in the Microsoft antitrust trial, *New York v. Microsoft*.

Steven M. Bellovin[33] is a Professor of Computer Science at Columbia University. He joined the faculty recently after many years at Bell Labs and AT&T Labs Research. He is an AT&T Fellow and a member of the National Academy of Engineering. Dr. Bellovin is the co-author of *Firewalls and Internet Security: Repelling the*

---

[31] PlanetLab Consortium, *at* http://www.planet-lab.org (last visited Feb. 6, 2005).

[32] Andrew W. Appel, Department of Computer Science, Princeton University, *at* http://www.cs.princeton.edu/~appel (last visited Feb. 6, 2005).

[33] Steven M. Bellovin, Department of Computer Science, Columbia University, *at* http://www.cs.columbia.edu/~smb (last visited Feb. 6, 2005).

Wily Hacker (2d ed. 2003) (with *amicus* Aviel Rubin, and Bill Cheswick) [hereinafter *Firewalls and Internet Security*], and holds several patents on cryptographic and network protocols. He has served on many National Research Council (NRC) study committees, and is a member of the Department of Homeland Security's Science and Technology Advisory Committee. He has been a member of the Internet Architecture Board and co-director of the Security Area of the Internet Engineering Task Force.

Dan Boneh[34] is a Professor of both Electrical Engineering and Computer Science at Stanford University. He heads the applied crypto group at the Computer Science department. Dr. Boneh's research focuses on applications of cryptography to computer security. He is the author of over 70 technical publications. His work includes digital copyright protection, e-mail security, security for handheld devices and web servers and cryptanalysis. He is a recipient of the Packard Award, the Alfred P. Sloan Award, and the Terman Award.

David Clark[35] is a Senior Research Scientist at MIT. More recent activities than those stated in the brief include extensions to the Internet to support real-time traffic, pricing and related economic issues, and policy issues surrounding the Internet, such as broadband local loop deployment. His current research looks at re-definition

---

[34] Dan Boneh, Department of Computer Science and Electrical Engineering, Stanford University, *at* http://theory.stanford.edu/~dabo (last visited Feb. 15, 2005).

[35] David Clark, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, *at* http://www.lcs.mit.edu/people/bioprint.php3?PeopleID=81 (last visited Feb. 6, 2005).

of the architectural underpinnings of the Internet, and the relation of technology and architecture to economic, societal and policy considerations. He is past chairman of the NRC's Computer Science and Telecommunications Board and a member of the National Academy of Engineering. Dr. Clark is a Fellow of the IEEE and of the ACM, and has won numerous awards for his work.

David J. Farber[36] is the Distinguished Career Professor of Computer Science and Public Policy at the School of Computer Science at Carnegie Mellon University with secondary appointments at the Heinz School and the Engineering and Public Policy Department of the College of Engineering. In 2003, he retired from the University of Pennsylvania where he held the Alfred Fitler Moore Chair of Telecommunications with appointments in the Engineering School and the Wharton School. From 2000-01, he served as Chief Technologist for the Federal Communications Commission. Prior to his appointment to the FCC, he served on the U.S. Presidential Advisory Committee on High Performance Computing and Communication, Information Technology, and the Next Generation Internet [hereinafter U.S. Presidential Advisory Committee on Information Technology]. He is a Fellow of the ACM and the IEEE, and serves on the Board of Directors of the Electronic Frontier Foundation. He is a member of the Markle Foundation Task Force on National Security in the Information Age.

[36] David J. Farber, School of Computer Science, Carnegie Mellon University, *at* http://www.epp.cmu.edu/people/bios/farber.htm (last visited Feb. 6, 2005).

Joan Feigenbaum[37] is a Professor in the Computer Science Department at Yale University. Prior to starting at Yale in 2000, she worked for AT&T, where she participated broadly in the company's Information-Sciences research agenda, e.g., by creating a research group in Algorithms and Distributed Data, of which she was manager in 1998-99. Dr. Feigenbaum's research interests include Internet algorithms, computational complexity, security and privacy, and digital copyright. While at Yale, she has been a principal in several high-profile activities, including the NSF-funded PORTIA (Privacy, Obligations, and Rights in Technologies of Information Assessment) Project and the Office of Naval Research-funded SPYCE (Stanford-Penn-Yale-Cornell Experiment) Project. Her current and recent professional service activities include Editor-in-Chief for the Journal of Cryptology, Program Chair for the 2002 ACM Workshop on Digital Rights Management, and Program Co-Chair for the 2004 ACM Conference on Electronic Commerce. Dr. Feigenbaum is a Fellow of the ACM.

Edward W. Felten[38] is a Professor of Computer Science at Princeton University. He is also affiliated with the Program in Science, Technology, and Environmental Policy, in the Woodrow Wilson School of Public and International Affairs, at Princeton. His research interests include computer security, Internet software, and information technology

[37] Joan Feigenbaum, Computer Science Department, Yale University, *at* http://cs-www.cs.yale.edu/homes/jf/home.html (last visited Feb. 6, 2005).

[38] Edward W. Felten, Department of Computer Science, Princeton University, *at* http://www.cs.princeton.edu/~felten (last visited Feb. 6, 2005).

policy. He is widely known for his research on anti-copying technologies. He has served in an advisory capacity to the U.S. Departments of Defense, Justice, and Homeland Security, and has testified before the Senate Commerce Committee regarding digital copyright policy. He was the primary computer science expert witness for the United States in *United States v. Microsoft*. Dr. Felten is a member of the Advisory Board of the Electronic Frontier Foundation.

Robert Harper[39] is a Professor of Computer Science at Carnegie Mellon University. His research is on programming language design and implementation. He is a principal co-designer of the Standard ML programming language and a co-inventor of the LF Logical Framework. He is Associate Editor for Programming Languages of the Journal of the ACM, the premier academic journal in computer science.

M. Frans Kaashoek[40] is a Professor in MIT's Electrical Engineering and Computer Science Department and a member of the Computer Science and Artificial Intelligence Laboratory, where he co-leads the parallel and distributed operating systems group. Dr. Kaashoek's principal field of interest is designing and building computer systems. His past work includes the exokernel operating system, the Click modular router, the Resilient Overlay Network, the self-certifying file system, and the

[39] Robert Harper, School of Computer Science, Carnegie Mellon University, *at* http://www-2.cs.cmu.edu/~rwh (last visited Feb. 15, 2005).

[40] M. Frans Kaashoek, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, *at* http://www.pdos.lcs.mit.edu/~kaashoek (last visited Feb. 6, 2005).

Chord protocol, a robust, scalable protocol to locate information in P2P systems. His current focus is the IRIS project. Dr. Kaashoek is the recipient of several awards, including the inaugural ACM Special Interest Group on Operating Systems' Mark Weiser award for demonstrating creativity and innovation in operating systems research.

Brian Kernighan[41] is a Professor in the Computer Science Department at Princeton University. Previously he was head of the Computing Structures Research Department at Bell Labs, where he did research in programming languages, software tools, and user interfaces. He is the co-author of a number of widely-used computer books and programs, and is a member of the National Academy of Engineering.

Jennifer Rexford[42] is a Professor in the Computer Science Department at Princeton University. Prior to February 2005, she spent eight years at AT&T Labs Research. Her research on network measurement, traffic engineering, and router configuration has led to several network-management tools that are in daily use in AT&T's IP backbone network. She is co-author of *Web Protocols and Practice: HTTP/1.1, Networking Protocols, Caching, and Traffic Measurement* (2001). She serves as the chair of ACM Special Interest Group on Data Communications, and is a member of the ACM Council, the Computing

[41] Brian Kernighan, Department of Computer Science, Princeton University, *at* http://www.cs.princeton.edu/~bwk (last visited Feb. 6, 2005).

[42] Jennifer Rexford, Department of Computer Science, Princeton University, *at* http://www.cs.princeton.edu/~jrex (last visited Feb. 6, 2005).

Research Association's Board of Directors, and DARPA's Information Science and Technology Study Group.

John C. Reynolds[43] is Professor of Computer Science at Carnegie Mellon University. He is a Fellow of the ACM and a recipient of the Lifetime Achievement Award from the ACM Special Interest Group on Programming Languages. He is also a member of International Federation of Information Processing Working Group 2.3 on Programming Methodology. His research centers on the design of languages for programming and the specification of programs, programming methodology, and methods for proving that programs meet their specifications.

Aviel D. Rubin[44] is a Professor of Computer Science and the Technical Director of the Information Security Institute at Johns Hopkins University. Prior to joining Johns Hopkins, Dr. Rubin was a scientist at AT&T Labs Research. Dr. Rubin is author of several books including *Firewalls and Internet Security* (co-authored with Bill Cheswick and *amicus* Steven M. Bellovin), *White-Hat Security Arsenal* (2001), and *Web Security Sourcebook* (1997) (co-authored with Dan Geer and Marcus Ranum). He is Associate Editor of IEEE Transactions on Software Engineering, Associate Editor of ACM Transactions on Internet Technology, Associate Editor of IEEE Security & Privacy, and an Advisory Board member of Springer's Information Security and Cryptography Book Series. Dr.

[43] John C. Reynolds, School of Computer Science, Carnegie Mellon University, *at* http://www-2.cs.cmu.edu/~jcr (last visited Feb. 6, 2005).

[44] Avi Rubin, Department of Computer Science, Johns Hopkins University, *at* http://www.cs.jhu.edu/~rubin (last visited Feb. 6, 2005).

Rubin serves on DARPA's Information Science and Technology Study Group.

Eugene H. Spafford[45] is a Professor of both Computer Sciences and of Electrical and Computer Engineering at Purdue University with courtesy appointments as Professor of Communication and as Professor of Philosophy. He is the founder and executive director of CERIAS, the Purdue Center for Education and Research in Information Assurance and Security, a national center of excellence and the nation's foremost academic center in this field. Dr. Spafford is a Fellow of the ACM, the IEEE, and the American Association for the Advancement of Science, and he was the year 2000 recipient of the NIST/NSA National Computer Software Security Award. He has been named to the Information Systems Security Association Hall of Fame, and has been awarded the William Hugh Murray medal from the National Colloquium for Information Systems Security Education for his contributions to research and education in information security. He is a recipient of the Air Force medal for Meritorious Civilian Service, is a recipient of the IEEE Computer Society's Taylor Booth medal, and of the ACM Special Interest Group on Computers and Society's "Making a Difference" award. He currently serves on the Computing Research Association's Board of Directors, and on the U.S. Presidential Advisory Committee on Information Technology, as well as many corporate advisory boards. Dr. Spafford has co-authored or edited 5 books, over 100 technical articles, holds 2 patents, and is the author of several software

[45] Eugene H. Spafford, Department of Computer Science, Purdue University, *at* http://www.cerias.purdue.edu/homes/spaf/narrate.html (last visited Feb. 18, 2005).

packages that have been the basis for commercial products.

David S. Touretzky[46] is a Research Professor of Computer Science at Carnegie Mellon University, and co-director of the graduate training program of the Center for the Neural Basis of Cognition. He has lectured on artificial intelligence, neural networks, and computational neuroscience in formats ranging from half-day industry seminars to semester-long graduate courses. Dr. Touretzky is also the author of a popular textbook on the Lisp programming language. He serves on the board of directors of the NIPS (Neural Information Processing Systems) Foundation, and is a member of the ACM and the American Association for Artificial Intelligence.

[46] David S. Touretzky, Computer Science Department, Carnegie Mellon University, *at* http://www-2.cs.cmu.edu/~dst (last visited Feb. 6, 2005).