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 UTAH, NORTH CAROLINA, VIRGINIA, RHODE ISLAND, TEXAS, MISSISSIPPI, ALABAMA, ALASKA, ARIZONA, ARKANSAS, DELAWARE, FLORIDA, GEORGIA, HAWAII, IDAHO, ILLINOIS, INDIANA, KANSAS, KENTUCKY, LOUISIANA, MASSACHUSETTS, MICHIGAN, MINNESOTA, MISSOURI, MONTANA, NEBRASKA, NEVADA, NEW JERSEY, NEW MEXICO, NORTH DAKOTA, OHIO, OKLAHOMA, PENNSYLVANIA, SOUTH CAROLINA, SOUTH DAKOTA, TENNESSEE, VERMONT, WEST VIRGINIA, WISCONSIN AND THE TERRITORY OF GUAM IN SUPPORT OF PETITIONERS

MARK SHURTLEFF*
ATTORNEY GENERAL OF UTAH
PO Box 142320
Salt Lake City, Utah
84114-2320
(801) 366-0300

ROY COOPER
ATTORNEY GENERAL OF NORTH CAROLINA
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400

Counsel for Amici Curiae

* Counsel of Record

January 24, 2005

[Additional Counsel Listed on Inside Cover and Front Pages]

JERRY KILGORE
ATTORNEY GENERAL OF
VIRGINIA
900 E. Main Street
Richmond, VA 23219
(804) 786-2071

PATRICK LYNCH
ATTORNEY GENERAL OF
RHODE ISLAND
150 S. Main Street
Providence, RI 02903
(401) 274-4400

GREG ABBOTT
ATTORNEY GENERAL OF
TEXAS
P.O. Box 12548
Austin, TX 78711-2548
(512) 463-2100

JIM HOOD
ATTORNEY GENERAL OF
MISSISSIPPI
Department of Justice
P.O. Box 220
Jackson, MS 39205-0220
(601) 359-3680

TROY KING
ATTORNEY GENERAL OF
ALABAMA
Alabama State House
11 South Union Street
Montgomery, AL 36130
(334) 242-7300

GREGG RENKES
ATTORNEY GENERAL OF
ALASKA
P.O. Box 110300
Juneau, AK 99811-0300
(907) 465-2133

TERRY GODDARD
ATTORNEY GENERAL OF
ARIZONA
1275 West Washington
Street
Phoenix, AZ 85007-2926
(602) 542-5025

MIKE BEEBE
ATTORNEY GENERAL OF
ARKANSAS
323 Center Street, Suite 200
Little Rock, AR 72201
(501) 682-2007

M. JANE BRADY
ATTORNEY GENERAL OF
DELAWARE
Carvel State Office
Building
820 N. French St.
Wilmington, DE 19801
(302) 577-8400

CHARLES J. CRIST, JR.
ATTORNEY GENERAL OF
FLORIDA
The Capitol PL-01
Tallahassee, FL 32399-1050
(850) 414-3300

THURBERT E. BAKER
ATTORNEY GENERAL OF GEORGIA
40 Capitol Square, SW
Atlanta, GA 30334-1300
(404) 656-3300

DOUGLAS B. MOYLAN
ATTORNEY GENERAL OF GUAM
Guam Judicial Center
120 W. O'Brien Drive
Suite 2-200E
Hagatna, GU 96910-5174
(617) 475-3324

MARK J. BENNETT
ATTORNEY GENERAL OF HAWAII
425 Queen Street
Honolulu, HI 9586-1500
(808) 586-1500

LAWRENCE G. WASDEN
ATTORNEY GENERAL OF IDAHO
700 W. Jefferson Street
P.O. Box 83720
Boise, ID 83720-0010
(208) 334-2400

LISA MADIGAN
ATTORNEY GENERAL OF ILLINOIS
James R. Thompson Center
100 W. Randolph Street
Chicago, IL 60601
(312) 814-3000

STEVE CARTER
ATTORNEY GENERAL OF INDIANA
IGCS—Fifth Floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 232-6201

PHILL KLINE
ATTORNEY GENERAL OF KANSAS
120 SW 10th Ave. 2nd Floor Topeka, KS 66612-1597
(785) 296-2215

GREGORY D. STUMBO
ATTORNEY GENERAL OF KENTUCKY
State Capitol, Suite 118
Frankfort, KY 40601
(502) 696-5300

CHARLES C. FOTI, JR.
ATTORNEY GENERAL OF LOUISIANA
P.O. Box 94005
Baton, Rouge, LA 70804
(225) 326-6000

THOMAS F. REILLY
ATTORNEY GENERAL OF MASSACHUSETTS
One Ashburton Place
Boston, MA 02108
(617) 727-2200

MICHAEL A. COX
ATTORNEY GENERAL OF MICHIGAN
P.O. Box 30212
Lansing, MI 48909
(517) 373-1110

MIKE HATCH
ATTORNEY GENERAL OF MINNESOTA
102 State Capitol
St. Paul, MN 55155
(651) 296-6196

JEREMIAH W. (JAY) NIXON
ATTORNEY GENERAL OF MISSOURI
Supreme Court Building
207 West High Street
P.O. Box 899
Jefferson City, MO 65102
(573) 751-3321

MIKE MCGRATH
ATTORNEY GENERAL OF MONTANA
Justice Building
215 N. Sanders. 3rd Street
P.O. Box 201401Helena, MT 59620-1401
(406) 444-2026

JON BRUNING
ATTORNEY GENERAL OF NEBRASKA
2115 State Capitol
P.O. Box 98920
Lincoln, NE 68509-8920
(402) 471-2682

BRIAN SANDOVAL
ATTORNEY GENERAL OF NEVADA
100 N. Carson Street
Carson City, NV 89701
(775) 684-1100

PETER C. HARVEY
ATTORNEY GENERAL OF NEW JERSEY
R.J. Hughes Justice Complex
25 Market Street
P.O. Box 080
Trenton, NJ 08625
(609) 292-4925

PATRICIA A. MADRID
ATTORNEY GENERAL OF NEW MEXICO
P.O. Drawer 1508
Santa Fe, NM 87504-1508
(505) 827-6000

WAYNE STENEHJEM
ATTORNEY GENERAL OF NORTH DAKOTA
State Capitol
600 E. Boulevard Avenue
Bismarck, ND 58505-0040
(701) 328-2210

JIM PETRO
ATTORNEY GENERAL OF OHIO
30 E. Broad St., 17th Floor
Columbus, OH 43215
(614) 466-8980

W.A. DREW EDMONDSON
ATTORNEY GENERAL OF OKLAHOMA
2300 N. Lincoln Boulevard
Suite 112
Oklahoma City, OK 73105-4894
(405) 521-3921

THOMAS W. CORBETT, JR.
ATTORNEY GENERAL OF PENNSYLVANIA
16th Floor, Strawberry Square
Harrisburg, PA 17120
(717) 787-3391

HENRY MCMASTER
ATTORNEY GENERAL OF SOUTH CAROLINA
P.O. Box 11549
Columbia, SC 29211-1549
(803) 734-3970

LAWRENCE E. LONG
ATTORNEY GENERAL OF SOUTH DAKOTA
500 East Capitol Avenue
Pierre, SD 57501-5070
(605) 773-3215

PAUL G. SUMMERS
ATTORNEY GENERAL OF TENNESSEE
P.O. Box 20207
Nashville, TN 37202-0207
(615) 741-3491

WILLIAM H. SORRELL
ATTORNEY GENERAL OF VERMONT
109 State Street
Montpelier, VT 05609-1001
(802) 828-3173

DARRELL V. MCGRAW, JR.
ATTORNEY GENERAL OF WEST VIRGINIA
1900 Kanawha Blvd., East
Room 26E
Charleston, WV 25305
(304) 558-2021

PEGGY A. LAUTENSCHLAGER
ATTORNEY GENERAL OF WISCONSIN
P.O. Box 7857
Madison, WI 53707-7857
(608) 266-1221

QUESTION PRESENTED

Whether the Ninth Circuit erred in concluding, contrary to long-established principles of secondary liability in copyright law (and in acknowledged conflict with the Seventh Circuit), that the Internet-based "file sharing" services Grokster and StreamCast should be immunized from copyright liability for the millions of daily acts of copyright infringement that occur on their services and that constitute at least 90% of the total use of the services.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES Page

TABLE OF AUTHORITIES—continued

TABLE OF AUTHORITIES—continued

TABLE OF AUTHORITIES—continued

OTHER AUTHORITIES

TABLE OF AUTHORITIES—continued

TABLE OF AUTHORITIES—continued

INTERESTS OF *AMICI CURIAE*

Amici States' and Territories' Attorneys General are responsible for enforcing the consumer protection, criminal, and other public interest statutes within their jurisdictions. Protecting the public and enforcing the law are central duties and obligations of the States. To these ends, *amici* seek to identify and prevent illegal conduct, to cultivate and encourage a culture of lawfulness, to protect consumers and to educate citizens about the laws that govern their conduct. The issues raised in this case implicate all of these important interests.

Of particular concern to *amici* is the need to promote and maintain a lawful business culture in which citizens and their institutions can safely use and benefit from rapidly advancing technological innovation. Critical to this effort are the well established legal doctrines of secondary liability which, both within and without copyright law, sanction and deter those—like respondents—who encourage and feed upon illegality. Given the importance of these doctrines generally, and to *amici* specifically in their role as law enforcement officers, this brief focuses upon general principles of secondary liability. It discusses the ways in which respondents' conduct falls squarely within long recognized principles of secondary liability and the ways in which permitting respondents to evade liability would undermine those same legal doctrines and foster lawlessness and an unaccountable business culture.

INTRODUCTION AND BACKGROUND

In order to appreciate fully the effect of the legal rule in this case, it is necessary first to consider the environment in which that rule will apply. The rule that this Court adopts will shape the use and abuse of file-sharing technology with regard to a variety of digital media by defining the manner in which secondary liability reaches illicit conduct in the online environment. Moreover, the rule will send an important signal that will shape the conduct of developers and distributors of new technology to the rule of law—a fact of critical importance to *amici* as law enforcement officers.

1. Respondents' peer-to-peer ("P2P") services are used overwhelmingly to locate and duplicate copyrighted works—including songs, movies, print and audio books and computer software—for free and without the permission of the copyright owners. In short, it enables massive copyright infringement. The scope of the unlawful conduct facilitated by respondents' activities is "mind-boggling." Pet. App. 65a-66a (congressional testimony of Marybeth Peters, Register of Copyrights). A recent survey reveals that 58% of Internet users use "a peer-to-peer network like Kazaa or Morpheus," or "have [done so] in the past."[1] More than 2.6 billion copyrighted songs are illegally downloaded from P2P networks each month, the equivalent of 200 million stolen CDs per month or 85 million songs per day. See Lev Grossman, *It's All Free*, Time, May 5, 2003. Simply put, "P2P networks have provided a sub-group of media consumers with the equivalent of a temporary repeal of copyright laws for the technologically inclined," Tim Wu, *When Code Isn't Law*, 89 Va. L. Rev. 679, 745 (2003), and the Ninth Circuit's decision in this case ratifies that repeal. This is crime of unprecedented scope and volume.[2]

The copyright infringement on which respondents' business is premised has real-world costs for American consumers and the economy. Illegal file sharing constitutes a significant

---

[1] Lee Rainie & Mary Madden, Pew Internet & American Life Project, *The State of Music Downloading & File-Sharing Online* 10 (Apr. 2004), *available at* http://www.pewinternet.org/pdfs/PIP_Filesharing_April_04.pdf.

[2] Indeed, P2P networks serve as the public distribution point for an extensive underworld of Internet piracy that steals copyrighted works, often before their public release, and races to distribute them for free. *See* Jeff Howe, *The Shadow Internet*, Wired Magazine (Jan. 2005), *at* http://www.wired.com/wired /archive/13.01/topsite_pr.html.

burden on the infrastructure of the Internet, as it constitutes more than half of total Internet traffic and consumes more than half of the bandwidth on the States' and Territories' university campuses.[3] In the copyright context, illegal file sharing victimizes artists, writers, production companies, distributors, theaters, and stores that do business lawfully in the States and Territories and, inevitably, the consumers of their products. Respondents' networks (and other P2P services that likewise follow an infringement-driven business model) have caused billions of dollars in lost sales. See Simon Dyson, Informa Media Group Report, *Music on the Internet* 25 (4th ed. 2003). And when legitimate commerce is submerged into a black market, the community loses jobs, business investment, and tax revenue that would otherwise be generated by the affected industry.[4]

These losses are not limited to brick-and-mortar businesses, but extend to online retailing, where the black market in copyrighted music has stunted the growth of legitimate music distribution over the Internet. Although several legitimate businesses have launched Internet sites that sell authorized

---

[3] Jeffrey Krauss, *Cable modem bandwidth management* (July 2003), *at* http://www.cedmagazine.com/ced/2003/0703/07cc.htm; Scott Carlson, *Napster Was Nothing Compared With This Year's Bandwidth Problems*, Chron. of Higher Educ., Sept. 28, 2001, at A44; Kenyon College, *Bandwidth Management at Kenyon*, *at* http://lbis.kenyon.edu/help/ntnetwork/bandwidth.phtml (last visited Jan. 21, 2005).

[4] *See* H.R. Rep. No. 105-339, at 4 (1997) (stating that the effect of electronic software theft "is substantial: 130,000 lost U.S. jobs, $5.6 billion in corresponding lost wages, $1 billion in lower tax revenue, and higher prices for honest purchasers of copyrighted software"); Business Software Alliance, *U.S. Software State Piracy Study* (Aug. 2003), *available at* http://www.bsa.org/globalstudy/2003_sps.pdf; James M. Sellers, Comment, *The Black Market & Intellectual Property: A Potential Sherman Act Section Two Antitrust Defense?*, 14 Alb. L.J. Sci. & Tech. 583, 604-06 (2004) (gathering data on the economic effect of copyright piracy, including online distribution of copyrighted works); Chris Taylor, *Invasion of the Movie Snatchers*, Time, Oct. 11, 2004, at A2 (noting that illegal downloads threaten a wide variety of artists).

downloads of songs and other materials,[5] the viability and success of these businesses is threatened because all of the copyrighted materials they sell can be obtained easily and quickly from respondents' P2P networks for free, see Jon Healey, *Sony BMG, Grokster Join Forces*, L.A. Times, Oct. 29, 2004, at C1 (according to the Chief of StreamCast Networks, "users are likely to abandon any file-sharing network that restricts their downloading in favor of the many networks that don't"). A rule of secondary liability that immunizes respondents' conduct will only ensure further losses and spread illegal conduct online, to the detriment of lawful businesses and the public.

To be sure, P2P technology is a potentially powerful tool for bringing people together in communities of shared interest. By enabling individuals directly to share information without regard to geography, P2P technology can open new avenues for businesses and government agencies to communicate and share information more effectively, for scientists and other researchers to more quickly and efficiently evaluate data and share insights, for individuals to share noncopyrighted material of historical, literary, or artistic significance, and for family members and friends to share recent photographs and other creations. See Cade Metz, *P2P Goes Private*, PC Magazine (Jan. 12, 2005), *at* http://www.pcmag.com/article2/0,1759,1746484,00.asp. *Amici* welcome this new tool for advancing human understanding and enriching the lives of our citizens. But, as with all new technology, *amici* are also keenly aware of its potential misuses and urge this Court to adopt rules that protect citizens

[5] *See, e.g.*, http://www.music.msn.com (music); http://www.apple.com/itunes (music, audio books, foreign language lessons and recorded public radio programs); http://www.amazon.com (print and audio books, audio newspapers such as *The New York Times*, music, recorded radio programs, and computer software); http://www.cinemanow.com (movies). Indeed, the threat of secondary copyright liability persuaded Napster to convert to a business based on authorized sales.

from crime, protect consumers from the effects of black markets and promote legal use of this powerful technology.

2. Of particular concern to the States is the widespread use of P2P networks illegally to distribute pornography, especially child pornography. "The trading of child pornography … on Gnutella, is rampant," as both the Justice Department and the GAO have recognized.[6] Furthermore, in a perverse effort to foist pornography upon unsuspecting underage computer users, pornographic materials are often disguised using file names that are meant to be attractive to young users, "such as 'Britney Spears,' 'Pokemon,' 'water sports,' or 'boy scouts.'" See Malcolm, *supra* note 6. A GAO study found: "In a search using innocuous keywords likely to be used by juveniles searching peer-to-peer networks … , almost half the images downloaded were classified as adult or cartoon pornography." *Koontz*, *supra* note 6, at 11. Many P2P users are ill-equipped to respond to this onslaught—41% of those who download files on P2P networks are between the ages of 12 and 18.[7]

Given respondents' affirmative disinterest in policing the networks they set in motion, and their reliance on conscious

[6] Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 Va. L. Rev. 505, 530 & n.92 (2003); Deputy Ass't Atty. Gen. John G. Malcolm, *Privacy and Intellectual Property—Legal Issues Related to Peer-to-Peer File Sharing Over the Internet*, Address to the N.Y. State Bar Ass'n & Int'l Bar Ass'n (Oct. 23, 2003), *available at* http://www.cybercrime.gov/Malcolmtestimony102303.htm; *File Sharing Programs, Users of Peer-to-Peer Networks Can Readily Access Child Pornography: Hearing Before the Subcomm. on Commerce, Trade & Consumer Protection of the House Comm. on Energy & Commerce*, 108th Cong. (testimony of Linda D. Koontz, Director, Information Management Issues, GAO), *available at* http://www.gao.gov/new.items/d04757t.pdf, at 2, 11.

[7] *The Dark Side of a Bright Idea: Will Personal and National Security Risks of P2P Networks Compromise the Promise of P2P Networks?: Hearing Before the Senate Comm. on the Judiciary*, 108th Cong. (2003) (statement of Sen. Hatch).

indifference to shield themselves from liability, see *infra* at 14-15, it is not surprising that their networks have become havens for other crime. These services are, for instance, rife with criminal schemes, such as instructions on how to pilfer financial accounting data from computer users and engage in electronic identity theft. Moreover, the use of hidden "spyware" (such as in Respondent Grokster's software), which is designed to monitor and report on the user's computer activities, violates consumers' privacy.

This illicit activity underscores the fact that the rule adopted by this Court is not limited, in its reach, to the realm of copyright. If respondents can evade responsibility for facilitating widespread copyright infringement simply by pretending not to know that it is occurring, then the creators of P2P networks that facilitate anonymous distribution of illicit pornography will believe they can do the same. Other P2P services will mimic respondents' successful behavior, thereby ensuring that they (and law enforcement officials, such as *amici*) know as little as possible about unlawful behavior on their networks in order to avoid secondary liability. P2P networks are demonstrably open to such abuse, and a rule of law concerning secondary liability that condones conscious disregard will promote such nefarious conduct, and will impede law enforcement from effectively combating it.

3. In the end, the most insidious consequence of respondents' business model may be the way it fosters networks of illegality. The P2P networks established by respondents and immunized by the Ninth Circuit rule promote a culture of lawlessness. Millions of people are engaged in illegal downloading via P2P services, see *supra* at 2 & n.1, and they believe that there is nothing wrong with doing so, see Wu, *supra,* at 722-26 (discussing studies showing that "those who use filesharing networks do not think they are stealing"); Strahilevitz, *supra*, at 581-82 (referring to "teenagers [who] have been socialized to believe that the copyright laws and the courts are largely ineffectual, and that

noncompliance with the spirit of the law is socially acceptable"). This is no accident—P2P software exploits ambiguity about whether the non-commercial copying of online music is wrong, and obfuscates the limitation of copyright law. Wu, *supra*, at 724. Given that one illegal act begets another, it is no surprise that respondents' P2P networks have spawned a culture of illegality on the Internet, as evidenced by the volume of infringement and the attitudes cited above.

It is a critical function of the law, and a responsibility of those who enforce it, to ensure a culture of general respect for the rights of others, and for the law itself. It is within such a culture that business can function, individual rights are respected, and consumers can be protected. Respondents' goal is just the opposite—to abet the development of networks of illicit conduct that pirate the work of copyright holders, and from which they can profit. This culture of illegality is condoned and substantially expanded by the decision below. The Ninth Circuit's rule provides an incentive for technological innovation to develop in a manner that ignores, and thus encourages, lawlessness. Its conclusion—that respondents' decision to eliminate or disable tools for detecting and discouraging illegal activity is *irrelevant* to the secondary-liability analysis—provides a perverse incentive for P2P businesses to eschew any available control over unlawful conduct on their networks, so that they can claim ignorance while garnering profit from the activity. In this regard, this case has no special application to technology, new technology or, for that matter, P2P technology. It is about enforcing fundamental principles of secondary liability against those who seek purposely to evade responsibility for the illegal conduct they set in motion.

SUMMARY OF ARGUMENT

This case turns on basic principles of secondary liability. Although it concerns a relatively new technology, that technology is merely the factual context in which age-old principles of secondary liability must be applied. Throughout the law, it is broadly recognized that those who aid, abet, or control the commission of a tort—or, for that matter, a crime—are just as liable as those who actually do the dirty work. Any individual who knows of and contributes to tortious activity, or controls and benefits from it, satisfies the two most basic prerequisites for liability: a guilty mind and a culpable act.

In the copyright context, as in the law generally, two distinct legal frameworks have evolved to capture these fundamental notions: contributory and vicarious liability. Both forms of secondary liability apply against respondents here. To hold otherwise would not only weaken the protections of copyright law, but of particular interest to *amici*, would weaken the legal mechanisms for imposing secondary liability against those who know of, enable, encourage and profit from the illicit conduct of others.

Contributory infringement, like aiding-and-abetting liability generally, applies when the defendant knows of the infringing acts of others, and induces, causes or materially contributes to those acts. Respondents' knowledge of infringement cannot be gainsaid—there is overwhelming evidence not only of their knowledge, but of affirmative intent. To be sure, they will respond that they were unaware that infringing conduct would occur on their networks; that they did not gain awareness at a legally sufficient moment; or, more surprising still, that they cannot be held liable because they do nothing more than distribute a neutral technology, any misuse of which must be laid at the feet of the end users. This defense is nothing more than a claim of willful blindness, which must be rejected here, just as it is throughout the law. A business that intends to profit from the illegal activity that it knowingly sets in motion cannot claim ignorance as an excuse.

Respondents also have materially contributed to the widespread infringement on their networks by making it possible. Indeed, their business model depends upon illegal activity—massive copyright infringement—which they not only knowingly facilitate, but intend to foster. Respondents derive advertising revenues that rise in value with the increased traffic on their networks. See *Metro-Goldwyn-Mayer Studios, Inc.* v. *Grokster*, 259 F. Supp. 2d 1029, 1044 (C.D. Cal. 2003). The more users they are able to attract with the prospect of free music or other copyrighted works, the more respondents can charge their advertising clients. Respondents have, therefore, made infringing conduct on their networks reliable, simple and fast. There is, of course, nothing inherently wrong with an ad-driven business model. Here, however, respondents have purposefully designed their business in a way that depends upon, and capitalizes upon, the rampant violation of the rights of others. Respondents' business model ought not be permitted to avoid secondary liability.

Vicarious liability applies, as here, when the defendant profits from the infringing acts of others, and has the right and ability to supervise and control the conduct. Respondents not only profit from the infringement in this case, but specifically depend upon it. Respondents claim no right or ability to control because they claim no connection to any individual acts of infringement. But respondents have chosen to offer access to P2P network software that makes infringement easy and quick, even though reasonable means are available to them to prevent or substantially reduce this foreseeable (indeed, intended) unlawful use of their networks. If respondents have no right to control their networks, it is because they have purposefully given it away. And while they certainly have the ability, they have chosen to operate in a way that disables such control. The rules of vicarious liability are broad enough to recognize that P2P network designers and software distributors effectively supervise and control the misconduct of their users under these circumstances.

ARGUMENT

I. IMPOSING LIABILITY FOR CONTRIBUTORY INFRINGEMENT IN THIS CASE IS CONSISTENT WITH LONGSTANDING PRINCIPLES OF AIDING-AND-ABETTING LIABILITY.

Basic principles of secondary liability, that are "recognized in every part of the law," *Kalem Co.* v. *Harper Bros.*, 222 U.S. 55, 63 (1911), properly resolve this case. Simply put, a party who knowingly contributes to tortious or criminal conduct is jointly and severally liable for the foreseeable consequences. See *Restatement (Second) of Torts* § 876(b) & cmt. d (1979); cf. also 18 U.S.C. § 2 (aiding and abetting liability under federal criminal law).

This general principle applies in the specific context of copyright law. *Gershwin Publ'g Corp.* v. *Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971) (contributory infringement is based on "'the common law doctrine that one who knowingly participates or furthers a tortious act is jointly and severally liable with the prime tortfeasor'"). It is embodied in a three-part test that both parties have agreed is applicable here: "[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer." *Id.* (footnote omitted).

There is no dispute that the requirement of underlying infringement is satisfied, nor could there reasonably be, given the millions of illicit copies of copyrighted works that have been made using respondents' software. See *supra* at 2. P2P networks for trading copyrighted materials have been called, without exaggeration, "arguably the largest international networks of illegality in human history," Strahilevitz, *supra*, at 507, and the record in this case indicates that approximately 90% of the works traded using respondents' networks are likely infringing, see Joint Appendix ("JA") 439. The questions, then, are whether respondents had "knowledge" of the infringing conduct, and whether they contributed to that infringement.

The manner in which this Court resolves these issues is of critical importance to *amici*. The undersigned Attorneys General are responsible for enforcing the majority of this Nation's consumer protection and criminal laws, many of which incorporate principles of secondary liability and, more fundamentally, include requirements of scienter and affirmative participation. That this case involves "new technology"—a mantra repeated by respondents throughout this litigation—is no defense to the very traditional ways in which respondents have aided and abetted unlawful conduct. To permit respondents to escape liability here would signal a radical departure from traditional legal principles and thereby impede consumer protection and law enforcement around the country.

A. Respondents Had Knowledge Of Infringement.

Under any reasonable legal standard, the evidence put forward by petitioners is more than sufficient to demonstrate that respondents had knowledge of the underlying infringement. The legal term "knowledge" differs little from its lay counterpart and means, simply, "[a]n awareness or understanding of a fact or circumstance." *Black's Law Dictionary* 888 (8th ed. 2004). A person "is said to act knowingly if he is aware '"that [a particular] result is practically certain to follow from his conduct, whatever his desire may be as to that result."'" *United States* v. *Bailey*, 444 U.S. 394, 404 (1980). Where the tort of aiding and abetting is concerned, of which contributory infringement is one variety, see *Sony Corp. of Am.* v. *Universal City Studios, Inc.*, 464 U.S. 417, 435 (1984); 1 Neil Boorstyn, *Boorstyn On Copyright* § 10.06[2], at 10-36.1 (2000), "it is enough for the aider and abettor to have a general awareness of its role in the other's tortious conduct for liability to attach," *Aetna Cas. &*

Sur. Co. v. *Leahey Constr. Co.*, 219 F.3d 519, 534 (6th Cir. 2000).[8]

In practical terms, this rule means that a jury may infer "that a person intends the natural and probable consequences of acts knowingly done or knowingly omitted." 1A *Federal Jury Practice and Instructions: Criminal* § 17.07, at 622 (5th ed. 2000). The same rule applies in the civil context. See *United States* v. *Peoni*, 100 F.2d 401, 402 (2d Cir. 1938) (L. Hand, J.) (recognizing secondary liability for the "natural consequence[s]" of one's actions); see also *Rice* v. *Paladin Enters., Inc.*, 128 F.3d 233, 251 (4th Cir. 1997) (recognizing that *Peoni*'s "natural consequence" standard speaks to scienter).

That standard is easily met, as there is abundant evidence from which a reasonable jury could conclude that respondents knew of the underlying infringement. Indeed, although such evidence need only be circumstantial, *Aetna*, 219 F.3d at 535; *FDIC* v. *First Interstate Bank of Des Moines, N.A.*, 885 F.2d 423, 430 (8th Cir. 1989); see also 1A *Federal Jury Practice and Instructions: Criminal* § 17.07, at 622, the record contains overwhelming direct evidence of knowledge.

First, the record reflects that respondents affirmatively intended to attract users who they knew would engage in copyright infringement. In the late 1990s and early 2000s, the foremost P2P network for enabling copyright infringement on the Internet was Napster. Copyright infringement on Napster was largely disabled in 2001 when the Ninth Circuit determined that Napster was likely engaged in contributory

[8] *Accord FDIC* v. *First Interstate Bank of Des Moines, N.A.*, 885 F.2d 423, 430 (8th Cir. 1989) ("the knowledge element is satisfied when the aider and abettor knows that the conduct of its principal is unlawful and that its own role is part of overall improper activity"); *Halberstam* v. *Welch*, 705 F.2d 472, 488 (D.C. Cir. 1983) (requiring showing of "general awareness"); *Wells Fargo Bank* v. *Arizona Laborers, Teamsters & Cement Masons Local No. 395 Pension Trust Fund*, 38 P.3d 12, 26 (Ariz. 2002).

and vicarious infringement, and enjoined Napster from permitting the "viral distribution" of copyrighted works. *A&M Records, Inc.* v. *Napster, Inc.*, 239 F.3d 1004, 1027 (9th Cir. 2001). Respondents not only intended their businesses to emulate Napster, but when Napster was enjoined from transferring copyrighted materials, respondents took affirmative steps to attract Napster's former users, including employing metatags with the word "Napster."[9] JA 738-739, 744-745, 749, 835, 836, 858-862, 864-865, 992-998. The CEO of StreamCast himself claimed that "[w]e have put this network in place so that when Napster pulls the plug on their free service (or if the Court orders them shut down prior to that) we will be positioned to capture the flood of their 32 million users that will be actively looking for an alternative." *Id.* at 861.

Napster's users were engaged in massive copyright infringement. Respondents' efforts to attract those users—in order to build and increase their user base, and thereby boost their advertising revenues—demonstrated not just *knowledge* of infringement on their networks, but the *intent* to attract infringers. Such intent satisfies the "knowledge" element of contributory infringement. *Bailey*, 444 U.S. at 404 ("purpose" shows greater culpability than "knowledge"); 1 Leonard B. Sand et al., *Modern Federal Jury Instructions: Criminal*, instr. 3A-1, at 3A-2 (2004) ("A person acts knowingly if he acts intentionally and voluntarily …."). At a minimum, widespread copyright infringement was a "natural

[9] A "metatag" is code on a web page that is invisible to the user, but visible to search engines, such as Yahoo! or Google. Thus, an Internet user employing Yahoo! to search for the term "Napster" would find not only the Napster web site itself (www.napster.com), but also web sites with the word "Napster" in its metatags, such as respondents'. *See Promatek Indus., Ltd.* v. *Equitrac Corp.*, 300 F.3d 808, 810 n.1 (7th Cir. 2002) (describing metatags).

and probable consequence" of attracting former Napster users to respondents' P2P networks.[10]

Second, respondents affirmatively sought to avoid gaining knowledge of the infringement to which they were contributing. Not only is such willful blindness no *defense* against knowledge, it constitutes affirmative *proof* of knowledge. As the Seventh Circuit recognized in the *Aimster* case, "Willful blindness is knowledge, in copyright law …, as it is in the law generally." *In re Aimster Copyright Litig.*, 334 F.3d 643, 650 (7th Cir. 2003) (citations omitted), *cert. denied*, 540 U.S. 1107 (2004). The reason is simple: "[A] deliberate effort to avoid guilty knowledge is all that the law requires to establish a guilty state of mind." *Id.* In the criminal context, too, it is uniformly recognized that "[i]n determining whether the defendant acted knowingly," a jury "may consider whether the defendant deliberately closed his eyes to what would otherwise have been obvious to him." 1 *Modern Federal Jury Instructions: Criminal*, instr. 3A-2, at 3A-5. Civil tort standards are not dissimilar. For instance, in the context of defamation, actual malice can be proved not only by actual knowledge of falsity, but also by "reckless disregard" of the truth, which is defined to include "evidence of an intent to avoid the truth." *Harte-Hanks Communications, Inc.* v. *Connaughton*, 491 U.S. 657, 693 (1989).

Here, the record demonstrates that respondents engaged in active avoidance of knowledge in a manner that "suggests that the[y] actually knew that [their] conduct was illegal and

---

[10] This evidence is a complete answer to the Ninth Circuit's conclusion that respondents were not on notice of the infringement until after they had already taken actions that furthered it. *Metro-Goldwyn-Mayer Studios, Inc.* v. *Grokster*, 380 F.3d 1154, 1162 (9th Cir. 2004). Respondents knew to a moral certainty *ab initio* that massive infringement would result, and intended that result, and accordingly had the requisite knowledge throughout the course of their actions in aid of the infringing conduct.

took measures to avoid the appearance of knowledge in order to claim lack of knowledge." 1 *Modern Federal Jury Instructions: Criminal*, instr. 3A-2 cmt., at 3A-7 & n.5. Respondents disabled a registration and login mechanism that required the use of a unique user name and password, and which had permitted them to control users' access to the P2P network and to deny access to users who violated the terms of the usage agreement. JA 254, 271-272, 575-578, 623-625, 626-628, 665-667, 766.

Were this not alone enough for a reasonable jury to infer that respondents sought to shield themselves from direct knowledge of infringement, the record indicates that respondents had precisely the purpose to avoid such knowledge. A StreamCast employee recognized that "If we have too much information on our users then we can be accused of having a Napster like relationship with them where we know what they are doing and specifically what they are listening to, that is when we are in jeopardy of legal pursuit." JA 791. Another StreamCast employee argued, for similar reasons, that the company should reject a proposal to purchase filtering technology: "What this is, is a technology that will allow Morpheus to see what our users are sharing so that in turn we can 'tie into a rights payment infrastructure.' I know this is something we DO NOT want to do, but am not sure how I need to word that." *Id.* at 928-933. To hold that this evidence is insufficient to establish liability—particularly given the procedural posture, in which all inferences must be drawn in petitioners' favor, see *Anderson* v. *Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986)—would validate respondents' efforts to shield themselves from knowledge.

Third, respondents were expressly aware that their networks were facilitating massive copyright infringement. The district court found that respondents "clearly know that many if not most of those individuals who download their software subsequently use it to infringe copyrights," 259 F. Supp. 2d at 1037, a conclusion that finds abundant support in the record. Respondents searched their own networks "for copyrighted song titles or artists." *Id.* at 1036; JA 532-535. StreamCast bragged to advertisers that a search of its network turned up far more songs by Madonna than a search of the service MP3.com. JA 936. A StreamCast executive complained when his search of a rival P2P network turned up more Garth Brooks songs than a search of their own network. *Id.* at 868. And respondents even advertised their product by touting the availability of copyrighted works. *Id.* at 821-826, 843-848, 889-893, 923-924, 936. This is precisely the sort of "invitation to infringement that … was missing in *Sony*." *Aimster*, 334 F.3d at 651.

What is more, petitioners repeatedly notified respondents of the massive infringement that was accomplished through use of their networks. 259 F. Supp. 2d at 1036; JA 176-179, 190-195, 199-200, 203-205, 235-239. Likewise, respondents were directly informed of infringement by consumers who used respondents' software to find and obtain copyrighted works. *E.g.*, *id.* 806 ("I used to use Napster all the time, and when they began battling in court I decided to look for a new place to look for all the music I love. I wanted to tell you that I have never had a problem finding any songs I want … its [sic] easy to find the latest tunes.").

Given the overwhelming evidence that respondents were actively aware of and intended the infringement that occurred over their networks, the defense recognized by this Court in *Sony* is inapplicable. In *Sony*, unlike this case, plaintiffs sought to impose liability for the mere sale of a product. Under those circumstances, this Court imported into copyright law a patent-law defense that applies when contributory infringement is alleged to result from the sale of a product—the "staple article of commerce" doctrine, which precluded liability because the product was "capable of substantial noninfringing uses," 464 U.S. at 442. The availability of that defense made sense under those circumstances, because an attack on the mere sale of a product implicates the public's interest in obtaining a new technology that is potentially infringing but also has beneficial uses. *Id.* at 440-42, 446.

But *Sony* did not apply that defense outside of the context of facial attacks on the sale of a technology, nor to a case—like this one—in which the defendants acted with knowledge or an intent to further infringement. And with good reason. In the patent context, that defense applies only under circumstances similar to those in *Sony*. See 35 U.S.C. § 271(c). It has no applicability whatsoever to the separate tort of "inducement of infringement," *id.* § 271(b), which closely mirrors contributory infringement in the copyright context, see *Water Techs. Corp.* v. *Calco, Ltd.*, 850 F.2d 660, 668 (Fed. Cir. 1988) (setting forth elements of inducement of infringement). In short, that defense would not apply here.

This limitation on the scope of the defense makes good sense. To afford its protection to those, like respondents, who knowingly or intentionally contribute to infringement, would amount to blanket amnesty for any deliberately contributing infringer who happens to sell a product with substantial noninfringing uses. Contributory infringers could brazenly announce their infringing purpose to the world—as respondents have done here—and there would be no consequence. That cannot be the rule, not only because of its absurdity, but because this Court has held that a defendant's intent is relevant to contributory infringement, see *Kalem*, 222 U.S. at 62-63 (considering the infringer's "purpose"), a rule that *Sony* seemingly reaffirmed, 464 U.S. at 438 n.18, 439 n.19 ("Sony certainly does not 'intentionally induc[e]' its customers to make infringing uses of respondents' copyrights" (alteration in original)).

B. Respondents Contributed To The Underlying Infringement.

1. There can be no question that respondents "materially contribute[d] to the infringing conduct," *Gershwin*, 443 F.2d

at 1162 (footnote omitted), of their P2P network users. This aspect of the contributory infringement analysis, like the knowledge element, can be resolved with simple reference to longstanding principles of secondary liability.

As with knowledge, "material[] contribut[ion]" finds uniform definition across civil and criminal law. The *Restatement (Second) of Torts* imposes liability upon a showing that the defendant "g[ave] substantial assistance or encouragement" to the principal tortfeasor." *Id.* § 876(b); *e.g.*, *Alleco Inc.* v. *Harry & Jeanette Weinberg Found., Inc.*, 665 A.2d 1038, 1049 (Md. 1995) (Maryland aiding and abetting law reaches anyone who "by any means encourage[s], incite[s], aid[s] or abet[s] the act of the direct perpetrator of the tort"). The analogous federal criminal statute similarly imposes principal liability upon one who "aids, abets, counsels, commands, induces or procures [the] commission" of a criminal offense. 18 U.S.C. § 2(a). This requirement, which "is well engrained in the law," is satisfied when "a defendant 'in some sort associate[s] himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed.'" *Nye & Nissen* v. *United States*, 336 U.S. 613, 618-20 (1949) (quoting *Peoni*, 100 F.2d at 402). "'[O]nce knowledge … is established, it does not take much to satisfy the facilitation requirement.'" 1 *Modern Federal Jury Instructions* instr. 11-2 cmt., at 11-13 to -14 & n.58.

In the civil context, the requirement of "substantial assistance or encouragement" is defined with further reference to five factors enumerated in the *Restatement*: "the nature of the act encouraged, the amount of assistance given by the defendant, his presence or absence at the time of the tort, his relation to the other and his state of mind." *Restatement (Second) of Torts* § 876 cmt. d; see *Halberstam* v. *Welch*, 705 F.2d 472, 481-84 (D.C. Cir. 1983). In the specific context of copyright, courts have recognized various forms of contribution. See, *e.g.*, *Fonovisa, Inc.* v. *Cherry*

Auction, Inc., 76 F.3d 259, 263 (9th Cir. 1996) (providing "the environment and market" in which counterfeiting thrives constitutes substantial assistance); *In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634, 652 (N.D. Ill. 2002) ("[d]efendants … have provided … software and … support services"), *aff'd*, 334 F.3d 643 (7th Cir. 2003).

Before evaluating the applicability of those factors here, it is important to note two circumstances present here that diminish the quantum of assistance that must be shown. First, the requirements of knowledge and substantial assistance "vary inversely relative to one another," so that "'where there is a minimal showing of substantial assistance, a greater showing of scienter is required,'" and vice versa. *Metge* v. *Baehler*, 762 F.2d 621, 624 (8th Cir.1985); *Woodward* v. *Metro Bank of Dallas*, 522 F.2d 84, 95 (5th Cir. 1975).[11] This commonsense principle applies with special force in this case, given the overwhelming evidence that respondents knew that their networks were being used principally as a vehicle for unlawful conduct; accordingly, not much in the way of an affirmative act shall be required. Second, the requirement of substantial assistance (and, likewise, the requirement of knowledge) is less strict "where the alleged aider and abettor derives benefits from the wrongdoing." *Gould* v. *American-Hawaiian S.S. Co.*, 535 F.2d 761, 780 (3d Cir. 1976).[12] Here,

---

[11] *Metge*, like several other cases cited here, concerned secondary liability under § 10(b) of the Securities and Exchange Act of 1934, 15 U.S.C. § 78j(b). Although this Court subsequently decided that there is no implied right of action for secondary liability under § 10(b), *see Central Bank of Denver, N.A.* v. *First Interstate Bank of Denver, N.A.*, 511 U.S. 164 (1994), that decision was purely a matter of statutory interpretation, and the § 10(b) secondary liability cases remain valid statements of the law of secondary liability, *see, e.g.*, *Aetna*, 219 F.3d at 535 (relying upon *Metge* after *Central Bank* was decided).

[12] *See also Metge*, 762 F.2d at 625-29 (considering the benefit to the party charged with secondary liability); *Woods* v. *Barnett Bank of Ft. Lauderdale*, 765 F.2d 1004, 1012 (11th Cir. 1985); *Armstrong* v. *McAlpin*, 699 F.2d 79, 91 (2d Cir. 1983); *Buttrey* v. *Merrill Lynch, Pierce, Fenner*

respondents not only "derive benefit" from the underlying infringement, the infringement is the cornerstone of their business model. Their business is structured to encourage a high volume of users engaged in illegal file sharing, so as to profit from increased advertising revenues. JA 72, 258, 572, 759-60.

2. The record in this case is replete with evidence of substantial assistance. First and foremost (and as further discussed below, see *infra* Section II.A.), respondents took numerous affirmative steps to design a system and distribute implementing software in order to facilitate infringement. Knowing full well that their system would attract Napster users in search of a new source of infringing materials, respondents distributed millions of copies of their software for free. That software provided the mechanism by which infringing conduct would occur. See *First Interstate Bank of Des Moines*, 885 F.2d at 433 (holding that serving as the means of transfer for illegal funds constitutes substantial assistance); but *cf. Metro-Goldwyn-Mayer Studios, Inc.* v. *Grokster*, 380 F.3d 1154, 1163 (9th Cir. 2004) (concluding, despite the evidence, that respondents "do not provide the 'site and facilities' for infringement"). They chose not to incorporate into that software any form of technology that might screen for infringing conduct, despite the availability of such technology.[13] They affirmatively disabled a registration

---

& Smith, Inc., 410 F.2d 135, 144 (7th Cir. 1969); *Wells Fargo*, 38 P.3d at 26 n.15, 27.

[13] 380 F.3d at 1163, 1165; JA 225-227, 228-232, 243-244, 275-285, 443; Darrell Smith, *The File-Sharing Dilemma*, CNet News (Feb. 3, 2004), *at* http://news.com.com/The+file-sharing+dilemma/2010-1027_3-5152265.html (StreamCast's former Chief Technology Officer admits that "there are no technical limitations to the ability to filter" out infringing files).

Contrary to the Ninth Circuit's decision, evidence of inaction is relevant to secondary liability. *See, e.g.*, *SEC* v. *Coffey*, 493 F.2d 1304, 1317 (6th Cir. 1974); *Brennan* v. *Midwestern United Life Ins. Co.*, 417 F.2d 147, 154-55 (7th Cir. 1969). And the compelling facts of this case—

mechanism that could be used to identify and disable infringers' access and, at a minimum, would deter such conduct. 380 F.3d at 1163; 259 F. Supp. 2d at 1040 n.7; JA 254, 271-272, 575-578, 623-625, 626-628, 665-667, 766. And they have repeatedly provided service for, and updates to, that software. JA 256, 260-261, 266-267, 269-270, 272-273. Given that contributory infringement is demonstrated by "contribution of machinery or goods that provide the means to infringe," 3 Melville Nimmer & David Nimmer, *Nimmer on Copyright* § 12.04[A][2], at 12-79 (2004), these facts surely defeat summary judgment. And they easily satisfy nearly every aspect of the *Restatement* test—respondents took actions that were directly relevant to the "nature of the act encouraged"; they provided assistance that was not merely substantial, but which provided the very mechanism by which the infringement was accomplished; and they engaged in an ongoing relationship with the infringers, with a culpable state of mind. *Restatement (Second) of Torts* § 876(b) cmt. d.[14]

Furthermore, respondents have affirmatively encouraged infringement over their networks. As noted above, respondents not only emulated the Napster network, but took numerous steps to attract Napster users. They advertised to

---

in which respondents disabled a registration mechanism to avoid knowledge of infringement, and declined to employ technologies to filter infringement—satisfy even the heightened standard for proof of inaction *qua* knowledge employed by some courts. *See, e.g.*, *Coffey*, 493 F.2d at 1317 ("[i]naction may be a form of assistance in certain cases, but only where it is shown that the silence of the accused aider and abettor was consciously intended to aid" the primary violation).

[14] For all of these reasons, the Ninth Circuit's conclusion is beside the point, even assuming it is true, that respondents' P2P networks could continue to function even if respondents' companies were shut down. 380 F.3d at 1163. The fact that the networks could function now says nothing about the substantiality of the assistance that respondents previously provided. Moreover, to conclude that it is insufficiently culpable to set in motion networks of infringement, so long as no control is maintained, would simply provide a perverse incentive for software developers to set loose networks of illegality that they cannot subsequently control.

the world that they provided the same service that the federal courts had just declared illegal on Napster's system. See, *e.g.*, 259 F. Supp. 2d at 1036 (respondents marketed their services as "'the next Napster'"); JA 836 (StreamCast promoted itself as "The #1 alternative to Napster"); *supra* at 12-14. And respondents encouraged infringement when they signaled that infringement was both possible and acceptable, by employing promotional materials that listed numerous songs and albums by well-known recording artists. JA 821-826, 843-848, 889-893, 923-924, 936. Such "encouragement" is specifically identified as satisfying section 876(b) of the *Restatement (Second)*, *see id.* cmt. d, as the case law confirms, see, *e.g.*, *Halberstam*, 705 F.2d at 481-82; see also *Sony*, 464 U.S. at 438 (relying on the district court's finding that Sony had *not* "influenced or encouraged" infringement).

Finally, this evidence of respondents' contributory actions is bolstered by respondents' intent to encourage and profit from infringement. See *supra* at 12-14. The *Restatement (Second)* looks specifically to the defendant's state of mind in considering substantial assistance, *id.* § 876(b) cmt. d, and this Court in *Sony* likewise indicated that an intent to induce illegal conduct is relevant to secondary liability, *supra* at 17. Respondents here, unlike those in *Sony*, not only "influenced [and] encouraged" their customers to engage in infringement; they "'intentionally induc[ed]'" them to do so. Such behavior establishes aiding-and-abetting liability throughout the law, and it does so here.

II. RESPONDENTS ARE VICARIOUSLY LIABLE FOR THE MASSIVE COPYRIGHT INFRINGEMENT THAT TAKES PLACE OVER THEIR NETWORKS.

For related, but conceptually distinct reasons, principles of vicarious liability also establish respondents' liability for the infringement on their networks. Because respondents profit from widespread infringement, have chosen to employ network software that makes infringing conduct easy and seemingly innocuous, and have rejected readily available technologies that would prevent or substantially diminish the frequency of infringement, they are vicariously liable.

The law has long recognized a three-part test to determine when to hold a defendant vicariously liable for copyright infringement, and that test is not in dispute here. There must be (1) direct infringement by the primary violator, (2) a direct financial benefit to the defendant, and (3) the right and ability to supervise the infringers. *Grokster*, 380 F.3d at 1164; 3 *Nimmer on Copyright* § 12.04[A][1], at 12-72. The first two parts of this test plainly are met, as the Ninth Circuit recognized—there are innumerable acts of primary infringement, and respondents generate substantial advertising revenue from the network traffic that itself results from easy consumer access to copyright-infringing materials. 380 F.3d at 1164. The Ninth Circuit nonetheless absolved respondents on the ground that they lack the right and ability to supervise the infringers. *Id.* at 1164-66. Its reasoning does not withstand scrutiny.

The Ninth Circuit viewed respondents' role in creating the networks that make massive copyright infringement possible as essentially like a landlord who does not supervise or control the actions of a tenant. Under traditional copyright law, such a landlord is not liable for the tenant's acts of infringement. *Id.* at 1164; 3 *Nimmer on Copyright* § 12.04[A][1], at 12-74 & nn. 23-27.3 (collecting cases). This limited view of respondents' role in the widespread illegality taking place on their networks is factually unsupportable and, moreover, it reflects a fundamentally flawed view of how P2P software technology affirmatively shapes the nature of the P2P network that it creates. The Ninth Circuit's rule thus allows companies to misuse P2P technology to profit from the legal evasions they make possible, evasions that potentially extend far beyond the copyright issues currently before the Court into areas such as the illicit distribution of child pornography.

This Court should reject the Ninth Circuit's view in favor of a commonsense approach that recognizes that respondents, when they make their network-creating software available to consumers, are neither indifferent to nor disassociated from the misconduct that takes place on the virtual communities they create. A P2P network designer or software distributor has the right and ability to supervise and control misconduct that it can reasonably foresee and which it can reasonably combat with available technology. It is precisely because respondents' software makes copyright infringement possible (and seemingly innocuous), despite the fact that they could reasonably equip it with the means to prevent or substantially diminish infringement, that respondents are "supervising and controlling" the misconduct that takes place on their networks. At an absolute minimum, and contrary to the Ninth Circuit's view, the ability to build protections against illicit conduct into the P2P network software is relevant to whether the software designer and distributor is liable for resulting infringement. Recognizing these principles would promote responsible business practices in the use of socially valuable P2P technology, and encourage respect rather than disdain for the rule of law and the rights of others.

A. Respondents Are Misusing The Powerful P2P Technology.

The misuse of P2P technology does not begin with the individual "peer" who chooses to enter a particular network. Rather, those who design P2P network software enable the network with specific abilities and limitations, and omit others; in that way, those who make the software available for users and maintain its efficient functioning exercise control over the conduct that takes place on the network. JA 442 ("The manner in which a software application operates is the result of innumerable conscious, affirmative decisions."). Software code, in effect, "regulates" the conduct of its users "by making [certain] behavior possible, or impossible." Lawrence Lessig, *Code and Other Laws of Cyberspace* 6, 89

(1999). P2P software can "define behavior on a mass scale." Wu, *supra*, at 707. And, of course, respondents are not indifferent to these design choices—as noted above, they derive substantial advertising revenue from design choices that permit illicit copying and thereby increase the volume of traffic on their networks.

In this case, respondents have chosen to define the behavior of their users in a number of ways. Respondents have incorporated technologies to prevent the copying of files containing viruses, or files that might appear to contain desirable content, but are actually "bogus" files that do not contain the data desired by the user. JA 253, 261, 274-275, 760. The sound business reasons for building a network with these filters are obvious—few people would use a network that placed them at high risk of receiving a harmful computer virus, or that too often failed to deliver the content that was requested. The installation of these devices, however, makes it clear that respondents are not simply providing a forum for users to deal directly with each other as they see fit; they are not, as the Ninth Circuit concluded, the equivalent of passive landlords. They are, rather, in the language of vicarious liability, "supervising and controlling" whether certain aspects of the content is and is not shared between users. It is true that no particular employee of respondents is "supervising or controlling" specific behavior in real time at the moment the files are shared and infringement takes place. Instead, the "supervision and control" take place at the code level, and it is no less effective—indeed, it is that much more so—for being designed into the P2P network itself.

In exercising this control, they affirmatively choose not to limit illicit file sharing. There is ample evidence in the record—particularly given the summary judgment posture—that respondents could just as easily have, at the code level, supervised and controlled (that is, prevented or substantially reduced) the sharing of copyrighted files. JA 225-227, 228-232, 243-244, 275-285, 443. They simply chose not to. On the contrary, they designed their services to take full advantage of the social ambiguity regarding whether the non-commercial copying of songs is "wrong." See Wu, *supra*, at 724; Holmes Wilson, *Defending the Families Sued by the RIAA* (Feb. 3, 2003), *at* http://www.kuro5hin.org/story/2003/10/16/14350/583 ("Not only does it not say anything about being illegal, Kazaa's site had 5 colored hearts across the top and looks like a toy."). And that choice, especially when combined with others respondents have made, has created a P2P community of lawbreakers who routinely infringe petitioners' copyrights. *Cf.* JA 789 ("What we have created with Morpheus at MusicCity.com is a community."). This stands in important contrast to the steps that other online businesses have taken to limit the illegal misuse of their technology. See, *e.g.*, Ariana Eunjung Cha, *Thieves Find Exactly What They're Looking For On Ebay*, Wash. Post, Jan. 6, 2005, at A01 (describing eBay's steps to identify and prevent the sale of stolen goods via its online auctions); *supra* note 5.

B. The Law Should Not Ignore The Fact That P2P Networks Can Be Equipped To Reduce Or Eliminate Illicit Conduct.

The Ninth Circuit held that respondents' ability to design and distribute P2P network software that would substantially diminish the incidence of infringement was legally irrelevant to respondents' vicarious liability. 380 F.3d at 1165-66. That ruling renders the law blind to business decisions that seek to profit from illicit conduct.

The illicit conduct in the present case is copyright infringement. Similarly, P2P networks also can generate profits for software distributors from the sharing of, for instance, child pornography. A rule that ignores the deliberate choice to disable control devices that might effectively prevent distribution of child pornography, or that might aid in tracking and prosecuting this predatory practice, should not receive approval from this Court.[15] This is particularly true, given that the standards for demonstrating criminal secondary liability are often more stringent than those for civil secondary liability. *Peoni*, 100 F.2d at 402. P2P networks can further profit by allowing users illegally and secretly to distribute spyware onto other users' computers, thus invading the privacy of users and potentially subjecting them to identity theft.[16] If a network software distributor can shield itself from liability merely by refusing to take reasonably available measures to prevent the reasonably foreseeable misuses of its network, and instead can profit from those misuses, then *amici* expect that the future will see the design of P2P software to facilitate the creation of more black markets that enable users, behind the

---

[15] In fact, some P2P networks disable control devices, such as user log-ins, that might be effective in tracking and prosecuting child pornography. As part of an ongoing effort to keep pace with emerging technologies that are being used to commit, facilitate and conceal Internet crimes against children, federal, state and local law enforcement officials have joined forces in a nationwide initiative to combat the large volume of child pornography being distributed through P2P networks. See Press Release, U.S. Immigration & Customs Enforcement, *Departments of Justice, Homeland Security Announce Child Pornography File Sharing Crack-down* (May 14, 2004), at http://www.ice.gov/graphics/news/newsreleases/articles/porncrackdown.htm. This effort is undermined and its success will be obstructed by a legal standard that permits companies that facilitate not only the conduct but also the anonymity of perpetrators, to escape any responsibility for their role in these crimes.

[16] Here, Grokster bundles the spyware program Cydoor with its software, which is automatically installed on the user's machine, albeit with the user's nominal consent. Cydoor displays pop-up advertisements and communicates information to advertisers about users' Internet activity. *CR Investigates: Protect Yourself Online*, Consumer Reports, Sept. 2004, at 12. Some sophisticated spyware is even capable of logging keystrokes to record personal information, such as online account passwords, which can lead to identity theft. Spyware consumes hard drive space, slows users' Internet connections and is responsible for a large percentage of computer crashes. *Id.*

anonymity of the Internet, to engage in illegal and socially harmful conduct.

There is no reason the law should ignore the ability to design and distribute software that includes reasonably available means to prevent the incidence of illicit transactions. As Judge Keeton has explained, the law generally recognizes that it is sound policy to place the responsibility for losses on the party who profits from misconduct, "even if that person makes arrangements for others to perform the acts that foreseeably cause the losses." *Polygram Int'l Publ'g, Inc.* v. *Nevada/TIG, Inc.*, 855 F. Supp. 1314, 1325 (D. Mass. 1994). The issue in this case is the right and ability to supervise and control the infringing conduct. *Amici* cannot perceive a clearer mechanism for supervision and control of illicit conduct than distributing P2P network software that *automatically* prevents acts of infringement. That is what respondents *could* do. That is what respondents *choose* not to do. For more than 40 years, courts have recognized that a department store has the ability to "supervise and control" infringing conduct merely because it contractually retains the right to exclude a vendor for any reason. *E.g.*, *Shapiro, Bernstein & Co.* v. *H.L. Green Co.*, 316 F.2d 304, 308-09 (2d Cir. 1963); *Fonovisa*, 76 F.3d at 262-63. It is difficult to see why the mere contractual right to exclude a vendor from one's premises, even in the absence of knowledge that infringement is taking place (as in *Shapiro*, 316 F.2d at 306), puts a department store owner in a greater position to supervise and control infringing conduct than a software designer and distributor who can take reasonable steps automatically to prevent infringing conduct from taking place.

This would not be the first time the law imposed a positive duty on commercial parties to include product features that reduce the risk of social harm. Products liability law recognizes that a product "is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor." *Restatement (Third) of Torts, Products Liability* § 2(b) (1998). This is a commonsense rule that encourages those who profit from the sale of goods to make sure that all reasonable efforts have been made to design the product in ways that will reduce the risk of foreseeable harm. *Id.* cmt. a (noting that a product should be judged in light of the knowledge of the risks and risk-avoidance techniques reasonably attainable at the time of distribution); *id*. cmt. f.

Similarly, those who control land (just as respondents have controlled the networks here, see *supra* Section II.A.) have a duty to their neighbors to take reasonable steps to prevent a third party from creating a nuisance on their land. See *Restatement (Second) of Torts* § 838 & cmts. e, g, illus. 3 (imposing such duties on "possessor[s]" of land); *id.* § 328E ("possessor" is defined by "control"). Importantly, this duty applies even as to third parties over whom the possessor *could* exercise control but chooses not to, *id.* § 838 illus. 5, 6 (so long as the means of control are not unreasonable, *id.* illus. 7)—which is precisely what respondents have refused to do here. The law should likewise require P2P network providers to take reasonably available steps to prevent infringement that they have reason to believe a third party will commit on their networks. And their failure to do so, when they know of, intend, and profit from the illicit uses, cannot be sanctioned.

It is worth repeating that *amici* do not seek to prevent the further development and use of P2P technology. We merely seek a clear rule of law that will promote the technology's socially beneficial uses, will foster respect for the law and rights of others, and will protect the consumers and economic welfare of our States and Territories. P2P software and services plainly can be developed that will both enable file sharing *and* respect copyright protections. Indeed, Grokster's own founder has announced plans to promote just such a network. David McGuire, *Mashboxx Aims to Make File*

Sharing Legit, Wash. Post, Dec. 22, 2004. Only if the law continues to insist upon respect for the rights of copyright owners will technology continue to develop along with respect for the law.[17] Adopting the rule for vicarious infringement proposed by *amici*, where the right and ability to control turns on the foreseeability of illicit conduct and the availability of reasonable means to inhibit it, will encourage both technology development and respect for the law.

CONCLUSION

For the foregoing reasons, the judgment of the Ninth Circuit should be reversed.

Respectfully submitted,

MARK SHURTLEFF*
ATTORNEY GENERAL OF UTAH
PO Box 142320
Salt Lake City, Utah 84114-2320
(801) 366-0300

ROY COOPER
ATTORNEY GENERAL OF NORTH CAROLINA
9001 Mail Service Center
Raleigh, NC 27669-9001
(919) 716-6400

---

[17] *See, e.g.*, May Wong, *TiVo Unveils Portable Transfer Service*, PC Magazine, Jan. 3, 2005 (reporting on new technology developed by TiVo that enables the transferable digital recording of television shows while respecting copyright law); Press Release, Google, *Google Checks Out Library Books*, Dec. 14, 2004, *at* http://www.google.com/press/pressrel/print_library.html (discussing Google project to digitize and place on the web the collections of research and public libraries, while respecting copyrighted material by refusing to make the full text of such material available online).

JERRY KILGORE
ATTORNEY GENERAL OF VIRGINIA
900 E. Main Street
Richmond, VA 23219
(804) 786-2071

PATRICK LYNCH
ATTORNEY GENERAL OF RHODE ISLAND
150 S. Main Street
Providence, RI 02903
(401) 274-4400

GREG ABBOTT
ATTORNEY GENERAL OF TEXAS
P.O. Box 12548
Austin, TX 78711-2548
(512) 463-2100

JIM HOOD
ATTORNEY GENERAL OF MISSISSIPPI
Department of Justice
P.O. Box 220
Jackson, MS 39205-0220
(601) 359-3680

TROY KING
ATTORNEY GENERAL OF ALABAMA
Alabama State House
11 South Union Street
Montgomery, AL 36130
(334) 242-7300

GREGG RENKES
ATTORNEY GENERAL OF ALASKA
P.O. Box 110300
Juneau, AK 99811-0300
(907) 465-2133

TERRY GODDARD
ATTORNEY GENERAL OF ARIZONA
1275 West Washington Street
Phoenix, AZ 85007-2926
(602) 542-5025

MIKE BEEBE
ATTORNEY GENERAL OF ARKANSAS
323 Center Street, Suite 200
Little Rock, AR 72201
(501) 682-2007

M. JANE BRADY
ATTORNEY GENERAL OF DELAWARE
Carvel State Office Building
820 N. French St.
Wilmington, DE 19801
(302) 577-8400

CHARLES J. CRIST, JR.
ATTORNEY GENERAL OF FLORIDA
The Capitol PL-01
Tallahassee, FL 32399-1050
(850) 414-3300

THURBERT E. BAKER
ATTORNEY GENERAL OF GEORGIA
40 Capitol Square, SW
Atlanta, GA 30334-1300
(404) 656-3300

DOUGLAS B. MOYLAN
ATTORNEY GENERAL OF GUAM
Guam Judicial Center
120 W. O'Brien Drive
Suite 2-200E
Hagatna, GU 96910-5174
(617) 475-3324

MARK J. BENNETT
ATTORNEY GENERAL OF HAWAII
425 Queen Street
Honolulu, HI 9586-1500
(808) 586-1500

LAWRENCE G. WASDEN
ATTORNEY GENERAL OF IDAHO
700 W. Jefferson Street
P.O. Box 83720
Boise, ID 83720-0010
(208) 334-2400

LISA MADIGAN
ATTORNEY GENERAL OF ILLINOIS
James R. Thompson Center
100 W. Randolph Street
Chicago, IL 60601
(312) 814-3000

STEVE CARTER
ATTORNEY GENERAL OF INDIANA
IGCS—Fifth Floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 232-6201

PHILL KLINE
ATTORNEY GENERAL OF KANSAS
120 SW 10th Ave. 2nd Floor Topeka, KS 66612-1597
(785) 296-2215

GREGORY D. STUMBO
ATTORNEY GENERAL OF KENTUCKY
State Capitol, Suite 118
Frankfort, KY 40601
(502) 696-5300

CHARLES C. FOTI, JR.
ATTORNEY GENERAL OF LOUISIANA
P.O. Box 94005
Baton, Rouge, LA 70804
(225) 326-6000

THOMAS F. REILLY
ATTORNEY GENERAL OF MASSACHUSETTS
One Ashburton Place
Boston, MA 02108
(617) 727-2200

MICHAEL A. COX
ATTORNEY GENERAL OF MICHIGAN
P.O. Box 30212
Lansing, MI 48909
(517) 373-1110

MIKE HATCH
ATTORNEY GENERAL OF MINNESOTA
102 State Capitol
St. Paul, MN 55155
(651) 296-6196

JEREMIAH W. (JAY) NIXON
ATTORNEY GENERAL OF MISSOURI
Supreme Court Building
207 West High Street
P.O. Box 899
Jefferson City, MO 65102
(573) 751-3321

MIKE MCGRATH
ATTORNEY GENERAL OF MONTANA
Justice Building
215 N. Sanders. 3rd Street
P.O. Box 201401Helena, MT 59620-1401
(406) 444-2026

JON BRUNING
ATTORNEY GENERAL OF NEBRASKA
2115 State Capitol
P.O. Box 98920
Lincoln, NE 68509-8920
(402) 471-2682

BRIAN SANDOVAL
ATTORNEY GENERAL OF NEVADA
100 N. Carson Street
Carson City, NV 89701
(775) 684-1100

PETER C. HARVEY
ATTORNEY GENERAL OF NEW JERSEY
R.J. Hughes Justice Complex
25 Market Street
P.O. Box 080
Trenton, NJ 08625
(609) 292-4925

PATRICIA A. MADRID
ATTORNEY GENERAL OF NEW MEXICO
P.O. Drawer 1508
Santa Fe, NM 87504-1508
(505) 827-6000

WAYNE STENEHJEM
ATTORNEY GENERAL OF
NORTH DAKOTA
State Capitol
600 E. Boulevard Avenue
Bismarck, ND 58505-0040
(701) 328-2210

JIM PETRO
ATTORNEY GENERAL OF
OHIO
30 E. Broad St., 17th Floor
Columbus, OH 43215
(614) 466-8980

W.A. DREW EDMONDSON
ATTORNEY GENERAL OF
OKLAHOMA
2300 N. Lincoln Boulevard
Suite 112
Oklahoma City, OK 73105-4894
(405) 521-3921

THOMAS W. CORBETT, JR.
ATTORNEY GENERAL OF
PENNSYLVANIA
16th Floor, Strawberry Square
Harrisburg, PA 17120
(717) 787-3391

HENRY MCMASTER
ATTORNEY GENERAL OF
SOUTH CAROLINA
P.O. Box 11549
Columbia, SC 29211-1549
(803) 734-3970

LAWRENCE E. LONG
ATTORNEY GENERAL OF
SOUTH DAKOTA
500 East Capitol Avenue
Pierre, SD 57501-5070
(605) 773-3215

PAUL G. SUMMERS
ATTORNEY GENERAL OF
TENNESSEE
P.O. Box 20207
Nashville, TN 37202-0207
(615) 741-3491

WILLIAM H. SORRELL
ATTORNEY GENERAL OF
VERMONT
109 State Street
Montpelier, VT 05609-1001
(802) 828-3173

DARRELL V. MCGRAW, JR.
ATTORNEY GENERAL OF
WEST VIRGINIA
1900 Kanawha Blvd., East
Room 26E
Charleston, WV 25305
(304) 558-2021

PEGGY A. LAUTENSCHLAGER
ATTORNEY GENERAL OF
WISCONSIN
P.O. Box 7857
Madison, WI 53707-7857
(608) 266-1221

Counsel for Amici Curiae

January 24, 2005

* Counsel of Record