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 OF KIDS FIRST COALITION, CHRISTIAN COALITION OF AMERICA, CONCERNED WOMEN FOR AMERICA, ENOUGH IS ENOUGH, MORALITY IN MEDIA, INC., NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, NATIONAL FRATERNAL ORDER OF POLICE, NATIONAL LAW CENTER FOR CHILDREN AND FAMILIES, AND WE CARE AMERICA AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

VIET D. DINH
Counsel of Record
CHRISTOPHER D. THUMA
BRIAN A. BENCZKOWSKI
BANCROFT ASSOCIATES PLLC
2121 Bancroft Place, N.W.
Washington, D.C. 20008
(202) 234-0090

Counsel for Amici

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20001

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 percent of the total use of the services.

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

CASES Page

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

MISCELLANEOUS Page

TABLE OF AUTHORITIES—Continued

INTERESTS OF *AMICI CURIAE*[1]

Amici are a variety of national, non-profit organizations broadly representing the interests of parents, children, and law enforcement officers. They share a commitment to the effective enforcement of the law, in particular prohibitions against child pornography, obscenity, and other predatory behavior against the Nation's children. *Amici* are concerned that the decision below will spawn a proliferation of anonymous, decentralized, unfiltered, and untraceable peer-to-peer networks that facilitate crimes against children and that frustrate law enforcement efforts to detect and investigate these crimes.

Kids First Coalition is a grassroots, non-profit organization of parents, grandparents, and future parents dedicated to advancing the interests of children and families and to educating the country about the needs of children. Penny Nance is the founder and president of Kids First Coalition. Membership includes parents from all walks of life throughout the United States. Kids First Coalition advocates on behalf of a variety of issues relating to children, including decency in broadcasting and on the Internet, alcohol regulation, the Innocence Protection Act, and other pro-family initiatives.

The Christian Coalition of America is a tax-exempt organization and one of the largest grassroots political groups in the country with over 2 million members. The orga-

---

[1] Petitioners and Respondents have consented to the filing of this brief. Consistent with Rule 37.6, this brief is not authored in whole or in part by counsel for any party. No person, other than *amici* or their counsel, has made a monetary contribution to the preparation or submission of this brief. Counsel of record is an independent, non-executive director of the News Corporation, parent company of Petitioner Twentieth Century Fox Film Corporation. Bancroft Associates PLLC provides ongoing public affairs and political strategy advisory services to the Recording Industry Association of America and the Motion Pictures Association of America, of which some Petitioners are members.

nization is involved in educating public officials and members of the community on important, pro-family issues of national concern. The Christian Coalition has played a particularly active role in state and federal efforts to enact laws regulating obscenity, child pornography, indecency, and materials that are harmful to minors.

Concerned Women for America is the nation's largest public policy women's organization. The organization provides policy analysis, legislative assistance and research for pro-family organizations. Concerned Women for America's research and publications on the impact of pornography have been distributed to scholars, organizations, and citizens across the country. The organization's Chief Counsel has also filed briefs with this Court on the subject of pornography.

Enough is Enough is a non-partisan, non-profit, educational organization dedicated to making the Internet safe for children and families. The organization is committed to raising public awareness regarding the dangers of Internet pornography and sexual predators, and advancing solutions that promote shared responsibility between the public, technology, and the law. Individuals involved with Enough is Enough come from varied backgrounds, professions, religions, non-profit organizations, and political affiliations.

Morality in Media, Inc., is a national, non-profit organization established in 1962 to combat obscenity and uphold decency standards in the media. Its public information and public affairs activities are designed to help individuals deal effectively and constitutionally with the threat of illegal pornography in their communities and the erosion of decency standards in the media. Morality in Media specializes in providing assistance on issues related to the laws of obscenity, child pornography, broadcast indecency, and the display and dissemination of materials that are harmful to minors. The organization regularly prepares proposed legis-

lation and administrative regulations, testifies before legislative and administrative bodies, and submits briefs *amicus curiae* in state and federal courts. Morality in Media also maintains the National Obscenity Law Center, a clearinghouse of legal materials on obscenity law.

The National Center for Missing and Exploited Children ("NCMEC") is a private, non-profit organization that provides services nationwide for families and professionals to prevent the abduction, endangerment, and sexual exploitation of children. Pursuant to its mission and congressional mandate (*see* 42 U.S.C. §§ 5771 *et seq.*; 42 U.S.C. § 11606; 22 C.F.R. § 94.6), NCMEC operates a CyberTipline that allows the public to report Internet-related child sexual exploitation and provides technical assistance to individuals and law-enforcement agencies in the prevention, investigation, and prosecution of cases involving missing and exploited children.

The National Fraternal Order of Police is the world's largest organization of sworn law enforcement officers, with more than 318,000 members in all 50 States. The organization is a non-profit corporation created to represent the interests of its members including participation as *amicus curiae* before this Court in matters in which the organization has unique expertise and insight. In particular, the organization understands the difficulties faced by law enforcement in the investigation of crimes involving child pornography.

The National Law Center for Children and Families is a non-profit corporation and educational organization specializing in legal issues related to obscenity, child pornography and sexual abuse, Internet regulations, and the display and dissemination of materials harmful to minors. Through training, advice, and legal research, the organization provides support on these issues to concerned citizens, local, state and federal government officials as well as law enforcement agencies across the United States. The Center has also filed

numerous briefs *amicus curiae* in this Court and in other federal and state courts.

We Care America is a faith-based organization dedicated to community development through governmental and private advocacy. We Care America sponsors initiatives to support needy children through adoption and foster care programs and provides avenues for various community volunteer opportunities.

STATEMENT OF THE CASE

Amici adopt the statement of the case presented in the Brief for Petitioner. For the Court's convenience, *amici* highlight below the facts most salient to the analysis that follows.

Peer-to-peer technology allows a member of an on-line network to access the computer files of other members. Because the accessible files are distributed throughout the members' computers, not stored in a centralized server, peer-to-peer software is necessary to catalogue available files, match the members' request with files, and connect the members to facilitate the file transfer. By linking information localized in individual computers into a network of global reach, peer-to-peer technology holds great potential for facilitating legal, productive activities.

Like any non-sentient, non-judgmental technology, peer-to-peer technology can be misused for illegal, pernicious activities. In *A&M Records, Inc.* v. *Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001), the court authorized an injunction against a peer-to-peer network for the illegal transfer of copyrighted works among its members if the network "knows or should know that such files are available" on the system and "fails to act to prevent viral distribution of the works." *Id.* at 1027. The relevant network in that case, Napster, maintained central servers to catalogue files available on its members' computers, to match its members' searches, and to connect the requesting "peer" to the offering "peer."

Napster's failure to prevent viral distribution of copyrighted works opened the network to secondary liability for its members' illegal trade in the works.

With the fall of Napster, peer-to-peer companies that were built on the same foundation—infringing content—had a choice: to act responsibly to prevent illegal activity or to turn in the opposite direction by taking steps to ensure that such illegal activity could continue to occur. Respondent StreamCast's own former Chief Technology Officer stated that "there are no technical limitations to the ability to filter" illegal content. Darell Smith, *The File Sharing Dilemma*, CNet News (Feb. 3, 2004), *available at* http://news.com.com/The+file+sharing+dilemma/2010-1027_35152265.html (last visited Jan. 21, 2005). It is not a question of "whether file-sharing companies can filter, but whether they will." *Id.*

Respondents Grokster and StreamCast took the opposite tack and disabled technologies to monitor and control network activities. They relocated their central server indices to the members' computers and decentralized the search function. They dismantled log-in and registration requirements and refused to install filtering software. *Metro-Goldwyn-Mayer Studios, Inc.*, v. *Grokster, Ltd.*, 380 F.3d 1154, 1165 (9th Cir. 2004) (hereinafter *Grokster II*). They then disclaimed responsibility for the content distributed over the network that they created and set out to target former Napster users deterred from the trade in illegal files.

Billing themselves as "the next Napster," Respondents' profited from the infringing activities of their users. *Metro-Goldwyn-Mayer Studios, Inc.* v. *Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1044 n.11 (C.D. Cal. 2003) (hereinafter *Grokster I*). As the District Court noted and Respondents do not dispute:

> StreamCast had $1.8 million in revenue in 2001 from advertising. And as of July of 2002, StreamCast had $2

> million in revenue and projects $5.7 million by the end of the year. Grokster also derives substantial revenue from advertising. The more individuals who download the software, the more advertising revenue Defendants collect. And because a substantial number of users download the software to acquire copyrighted material, a significant proportion of Defendants' advertising revenue depends upon the infringement. Defendants thus derive a financial benefit from the infringement.

Id. at 1044 (internal citations omitted).

Petitioners are U.S. motion picture studios, record companies, and a certified class of 27,000 music publishers and songwriters. Petitioners sought an injunction against continuing copyright infringement on the Grokster and StreamCast services based on contributory and vicarious infringement theories of copyright liability. The District Court granted summary judgment for Respondents. *Grokster I*, 259 F. Supp. 2d at 1046.

The Court of Appeals for the Ninth Circuit affirmed. *Grokster II*, 380 F.3d at 1167. The Ninth Circuit recognized that the Grokster and StreamCast software "enables the user to participate in the respective peer-to-peer file-sharing networks," *id.* at 1160; that "the vast majority of the files are exchanged illegally in violation of the copyright law," *id.*; that Grokster and StreamCast know their systems are being used for infringement; and that they profit handsomely from, and in direct proportion to, the level of infringement, *id.* at 1160, 1164.

Despite these undisputed facts, the court concluded that Grokster and StreamCast did not materially contribute to the infringement because they did not possess the "right and ability to supervise" and control the behavior of its users. *Id.* at 1164-65. The Ninth Circuit also rejected Petitioners' claim that Respondents should be held liable because they refused to take steps to monitor the behavior of their users. *Id.*

Finally, the Ninth Circuit dismissed the argument that Grokster and StreamCast should not be able to escape vicarious liability by simply turning a "blind eye" to the copyright infringement of their users while simultaneously relying on that activity in order to be profitable. *Id*. at 1166.

The decision below stands in contrast to *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003). The Seventh Circuit there rejected the efforts of the software designers to blind themselves to illegal activity. *Id.* at 650. *Aimster* involved a peer-to-peer system that used encryption in an attempt to disclaim responsibility for the illegal activity on its network. *Id.* at 646, 649. Although the encryption prevented Aimster from obtaining actual knowledge of specific infringement, Judge Posner recognized that "a deliberate effort to avoid guilty knowledge is all that the law requires to establish a guilty state of mind." *Id*. at 650. What matters for contributory liability is not artfully evasive structuring of the network, but rather the magnitude of infringing and non-infringing uses for the software. *Id.* at 649-50.

SUMMARY OF ARGUMENT

Respondents designed their business and deployed their technology to evade the requirements of law. In *Napster*, the Ninth Circuit authorized an injunction against a peer-to-peer network—similar to that owned by Respondents—in part for failure to detect and stop infringement. 239 F.3d at 1024, 1029. By redesigning their business model and software so that they could disclaim any knowledge or control over distributed content, Respondents sought to profit from the illegal activity as the "next Napster." *Grokster I*, 259 F. Supp. 2d at 1044 n.11.

The Ninth Circuit's decision to endorse Respondents' evasive strategy has implications far beyond that of copyright law. The decision below shelters not only illegal copyright infringement, but gives sanctuary to the distribution of child pornography and obscenity and other illegal activity con-

ducted on peer-to-peer networks. In alarming numbers, pedophiles are using peer-to-peer systems to trade in illicit material other than copyrighted works. *See* S. Rep. No. 106-141, 106th Cong., 1st Sess., at 3 (1999); *Online Pornography: Closing the Doors on Pervasive Smut*, Hearing Before the House Subcommittee on Commerce, Trade, and Consumer Protection, 108th Cong. (May 6, 2004) (statement of Penny Nance, President, Kids First Coalition). Identity thieves and malicious hackers are similarly drawn to the anonymity and lack of accountability that these networks provide. *See* Staff of House Comm. on Government Reform, Report Prepared for Rep. Tom Davis and Rep. Henry A. Waxman, 108th Cong., *File-Sharing Programs and Peer-to-Peer Networks Privacy and Security Risks* at 1, 5-9 (Comm. Print May 2003) (hereinafter *Privacy and Security Risks*). The Ninth Circuit's decision encourages network architects to blind themselves to such unlawful content and discourages the detection and prevention of illegal activity.

The decision below is an anomaly among traditional principles of secondary liability in copyright law. Courts have consistently allocated responsibility for copyright infringement to those who have an ongoing relationship with the direct infringer. *See Sony Corp. of America* v. *Universal City Studios, Inc.*, 464 U.S. 417, 437 (1984). Respondents' ability to update their software and otherwise maintain contact with their customers demonstrates such a relationship. The Ninth Circuit adopted a false analogy to a manufacturer that sells a product and loses all control over its use. *See Grokster II*, 380 F.3d at 1160-61. Respondents, however, are not limited in filtering infringing use by any technological barrier, but rather by conscious choice.

These concepts of copyright secondary liability that the Ninth Circuit ignores general concepts of secondary liability from other areas of law, such as property, tort, criminal, and corporate law. The law has consistently taken a dim view of owners who fail to end illegal use of their property, or who

take actions which increase the likelihood of illegal activity. Respondents did not merely abdicate their responsibility to prevent illegal activity, but took affirmative steps to facilitate illegal acts on their networks and benefited from those illegal acts. Holding Respondents responsible for the illegal use of the their networks is no different than ensuring that a landowner does not allow tenants to use property illegally, holding a store owner responsible for maintaining a safe workplace.

ARGUMENT

I. BY SANCTIONING RESPONDENTS' STRATEGY TO EVADE LEGAL LIABILITY, THE DECISION BELOW PROVIDES SANCTUARY FOR ILLEGAL ACTIVITY SUCH AS THE DISTRIBUTION OF CHILD PORNOGRAPHY, OBSCENITY, AND OTHER PROHIBITED MATERIALS.

Respondents designed their business and deployed their technology to evade the requirements of law. *Napster* authorized an injunction against a peer-to-peer network in part because it employed a centralized server and search engine. 239 F.3d at 1023-24. Respondents structured their business and technology to evade that ruling. By designing their software so that they could disclaim any knowledge or control over distributed content, they hoped to continue to profit from illegal activity as the "next Napster." *Grokster I*, 259 F. Supp. 2d at 1036, 1044 n.11.

The Ninth Circuit's endorsement of engineered ignorance of use and content carries consequences far beyond copyright law. The decision below shelters file-sharing networks from copyright liability, but its reasoning encourages network architects to design their systems deliberately to disclaim

knowledge of or control over other illegal conduct. The decision encourages peer-to-peer networks to blind themselves to distributed content and to avoid detecting and filtering illegal, pernicious activities such as the trafficking of child pornography and obscenity.

A. The Decision Below Sanctioned Respondents' Evasion of Law and Encourages the Development of Anarchic Networks.

The central question in this litigation is whether a network owner can divest liability for illegal activity facilitated by its service simply by structuring its business plan, legal instruments, and technology choices to disclaim any supervision or control over such illegal activity. The Ninth Circuit disaggregates its reasoning into two theories of liability, contributory and vicarious, each with its own three subparts—respectively, "(1) direct infringement by a primary infringer, (2) knowledge of the infringement, and (3) material contribution to the infringement," *Grokster II*, 380 F.3d at 1160, and "(1) direct infringement by a primary party, (2) a direct financial benefit to the defendant, and (3) the right and ability to supervise the infringers," *id.* at 1164. There is no dispute, however, that there is direct infringement by Grokster and Streamcast members, *Grokster I*, 259 F. Supp. 2d at 1034, that the networks know that over 90 percent of their traffic is for infringing use, *Grokster II*, 380 F.3d at 1157, and that they profit from advertising revenue derived from such traffic. *Grokster I*, 259 F. Supp. 2d at 1036, 1044 n.11. According to the decision below, the remaining third prongs of either theory of liability are simply two sides of the same coin, for a network owner materially contributes to infringement if it fails to stop the known infringement, *Grokster II*, 380 F.3d at 1163, and is vicariously liable if it does not exercise the right and ability to supervise its network against illegal conduct. *Id.* at 1164-65.

The Ninth Circuit absolved Respondents of legal liability because they have adopted business, legal, and technological strategies that disclaim any right and ability to supervise their network and thus to monitor or stop illegal conduct. Napster was liable, so goes the reasoning, because it operated "an integrated service" and "because it controlled the central indices of files, users were required to register with Napster, and access to the system depended on the validity of a user's registration." *Id.* at 1165 (citing *Napster*, 239 F.3d at 1011-12, 1023-24); *see also Grokster II*, 380 F.3d at 1163 (same for material contribution).

Grokster, by contrast, is not liable because even though it "nominally reserves the right to block access to individual users," it does not exercise that right "given the lack of a registration and log-in process." *Grokster II*, 380 F.3d at 1165. Moreover, "its licensing agreement with KaZaa/ Sharman does not give it the ability to mandate that root nodes be shut down." *Id.* Thus, Grokster bears no legal responsibility for the design of its business, legal, and technological structure after it releases the network software because "possibilities for upgrading software located on another person's computer are irrelevant to determining whether vicarious liability exists." *Id.* at 1166.

These business, legal, and technological distinctions did not arise by happenstance, but rather reflect Respondents' effort to evade legal requirements. Respondents' systems initially operated using the same centralized index server concept that Napster employed. After the *Napster* injunction, they reprogrammed their software to hijack members' computers to serve as decentralized indexing nodes. JA 279-86 (Kleinrock declaration).[2] Likewise, Respondents initially required individualized registration with a username and

[2] All citations to record evidence are to the Joint Appendix ("JA") before the Ninth Circuit.

password. JA 1096, 574-77. During this litigation, Respondents eliminated the log-in feature and thereby disclaimed any ability to deny access. Finally, Respondents initially had user agreements in which they reserved the right to terminate members' access to the networks. JA 340-43, 1005-07. During this litigation, StreamCast renounced this reservation and Grokster denied any enforcement capacity.

The Ninth Circuit blithely dismissed the import of these evasive maneuvers because "[t]he technology has numerous other uses, significantly reducing the distribution costs of public domain and permissively shared art and speech, as well as reducing the centralized control of that distribution." *Grokster II*, 380 F.3d at 1164. But surely a person's numerous innocent reasons for driving down the street in no way excuse his failure to pull over when followed by a police car with its lights flashing.

Consider the breathtakingly perverse implications of the Ninth Circuit's reasoning. The classic swap meet owner liable for the trade in infringing products on his premises, *Fonovisa, Inc.* v. *Cherry Auction*, 76 F.3d 259, 261 (9th Cir. 1996), can divest legal liability simply by eschewing "the ability to exclude individual participants [and] a practice of policing the aisles," *Grokster II*, 380 F.3d at 1165. The dance hall operator—another classic case of secondary liability, *id*. at 1164-65—can absolve liability by throwing the doors open to brigands and thieves. He can even profit by selling as much liquor as he wants, provided that he has disclaimed any responsibility to stop serving alcohol under any conditions. It defies law and logic that, by opening the doors wider to illegal activity, the property owner absolves himself of legal liability.

The decision below is not only perverse, it is pernicious. The owners' engineered ignorance of the content distributed over their networks extends not only to copyright works, but

also to illegal distribution of other prohibited materials, such as child pornography and obscenity. A system that blinds itself to infringement also blinds itself to the illegal transfer of other prohibited materials. Conversely, a responsible network that implements systems to monitor, prevent, and assist law enforcement prosecute distribution of prohibited materials stands at a commercial disadvantage to its competetors operating under the Ninth Circuit's legal sanctuary.

It is of little moment that Respondents have employed a search filter purportedly to weed out untoward searches. Whenever a user enters certain search terms—for example, "nude"—a dialogue box pops up asking whether the user would like to turn off the adult screening function and continue with the search. The "filter" thus functions more as an alert for inadvertent searches rather than a screening filter. More important, Respondents have restructured their system to disable any effective screen or filter of illegal use or content—as "none of the communication between defendants and users provides a point of access for filtering or searching for infringing files, since infringing materials and indexing information do not pass through defendants' computers." *Grokster II*, 380 F.3d at 1165. Such engineered futility facilitates illegal activity on a "mind-boggling"[3] scale; the decision below sanctions a safe haven for such unfettered illegal activity.

By sanctioning Grokster's conduct, the Ninth Circuit has effectively shielded the provider of an ignorant network from any form of culpability, whether civil or criminal. The closest analogue in the criminal context to secondary civil liability is the law of aiding and abetting. *Aimster*, 334 F.3d at 651. The law of aiding and abetting requires more than

[3] *Statement of the Honorable Marybeth Peters, Register of Copyrights*, Hearing Before the Senate Committee on the Judiciary, 108th Cong. (Sept. 9, 2003).

simply providing a means or a component necessary for the completion of an unlawful activity. As Judge Learned Hand explained, it requires that the alleged aider and abettor "in some sort associate 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." *United States* v. *Peoni*, 100 F.2d 401, 402 (2d Cir. 1938). This requires both knowledge of the intended unlawful activity and material assistance in that venture in an effort to help it succeed. *See, e.g., United States* v. *Pino-Perez*, 870 F.2d 1230, 1235 (7th Cir. 1989) (*en banc*). If a network provider can disavow civil liability simply by constructing a network of ignorance, it follows, *a fortiori*, that criminal liability cannot attach. The Ninth Circuit decision simply ignores the longstanding and common sense rule that "a deliberate effort to avoid guilty knowledge is all that the law requires to establish a guilty state of mind." *Aimster*, 334 F.3d at 650; *see generally* David Luban, *Contrived Ignorance*, 87 Geo. L.J. 957, 959 (1999).

B. The Decision Below Encourages the Proliferation of Irresponsible Networks that Facilitate Unfettered Distribution of Illegal Materials.

The failure of regulatory mechanisms to curb illegal uses of peer-to-peer networks, of which the decision below stands as the preeminent example, has denigrated this valuable technology to its lowest form. "Peer-to-peer facilitates the most extreme, aggressive and reprehensible types of behavior that the Internet will allow." Audrey Gillan, *Race to Save New Victims of Child Porn*, The Guardian, Nov. 4, 2003 (quoting David Wilson, professor of criminology at the University of Central England), *available at* http://www.guardian.co.uk/child/story/0,7369,1077260,00.html (last visited Jan. 21, 2005).

These networks place children at serious risk of physical harm. Congress, in passing the Child Internet Protection Act

("CIPA"), documented increasing incidents of professional pedophiles using the Internet to prey on children. "[A]n increasingly disturbing trend is that of highly organized, and technologically sophisticated groups of pedophiles who utilize advanced technology to . . . sexually exploit and abuse children." S. Rep. No. 106-141, at 3-4 (1999). The Internet and other on-line services are "one of the most prevalent techniques by which pedophiles and other sexual predators" identify "children for sexually explicit relationships." *Legislative Proposals to Protect Children from Inappropriate Materials on the Internet*, Hearing Before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the House Committee on Commerce, 105th Cong. 26 (1998) (statement of Stephen R. Wiley, Chief, Violent Crimes and Major Offenders Sections, Federal Bureau of Investigation).

Disturbingly, peer-to-peer networks are becoming the preferred method to transfer child pornography. The United States General Accounting Office ("GAO") recently concluded that peer-to-peer networks are quickly emerging as a major conduit for the distribution of child pornography.[4] U.S. General Accounting Office, Report GAO-04-757T, *File Sharing Program: Users of Peer-to-Peer Networks Can Readily Access Child Pornography*, at 2, 11 (May 6, 2003) (hereinafter GAO Report 1). In one search of peer-to-peer networks using 12 keywords known to be associated with child pornography on the Internet, GAO identified 1,286 titles and file names, determining that 543 (about 42 percent) were

[4] *See* 18 U.S.C. §§ 2251-52 (2004) (prohibiting the creation, possession, transport, sale, distribution, receipt, and advertisement of child pornography); 18 U.S.C. §§ 1460-70 (2004) (prohibiting the transportation, transmission, and sale of obscene material). Child pornography is unprotected by the First Amendment. *See New York* v. *Ferber*, 458 U.S. 747 (1982). Nor do First Amendment protections extend to the production, distribution, or transfer of obscene material. *See Roth* v. *United States*, 354 U.S. 476 (1957).

associated with child pornography images. *Id.* Of the remaining, 34 percent were classified as adult pornography and 24 percent as non-pornographic. In another search using three keywords, a U.S. Customs analyst downloaded 341 images, of which 149 (about 44 percent) contained child pornography. *Id.* Similarly, a congressional report noted that the sixth most popular search on one peer-to-peer network was the word "teen" and the eighth most popular was "preteen." Special Investigations Division, Minority Staff of House Comm. on Government Reform, 107th Cong., *Children's Access to Pornography Through Internet File-Sharing*, at 5 (Comm. Print 2001).

The National Center for Missing and Exploited Children ("NCMEC") has found that peer-to-peer technology is increasingly popular for the dissemination of child pornography. GAO Report 1 at 2, 11. The technology makes it easier to distribute, hide, and access illicit images and videos. *Id.* Peer-to-peer technology enables pedophiles to download larger files—for example, a 10-minute movie with sound—which they cannot easily obtain through websites or email. *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues*, Hearing Before the Federal Trade Commission, at 84 (Dec. 15, 2004) (statement of Michelle Collins, Director of the Exploited Child Unit of the National Center for Missing and Exploited Children), *available at* http://ftc.gov/bcp/workshops/filesharing/transcript_041215.pdf (last visited Jan. 21, 2005). Accordingly, reports to NCMEC of child pornography on peer-to-peer networks increased more than fivefold from 2001 to 2003. GAO Report 1 at 2, 11. In 2004, the Center received 39 percent more reports of suspected child pornography than it did the previous year, due in part to the increasing popularity of peer-to-peer networks.[5]

[5] Reports of child pornography to the Center have increased every year since the organization established a 24-hour hotline in 1998 to collect tips on child exploitation. John Foley, *Reports of Child Pornography*

National Center for Missing and Exploited Children, *Cyber Tipline: Annual Report Totals by Incident Type: January 1, 1998 to December 31, 2004* (2005).

Anonymous peer-to-peer networks—of the type that Respondents engineered to evade the *Napster* decision—present a particularly acute problem. The absence of registration on peer-to-peer networks conceals pedophiles' efforts to identify, lure, and seduce children into illegal and abusive sexual activity. S. Rep. No. 106-141, at 3 (1999). Many pedophiles believe it is harder for them to be detected on peer-to-peer networks as opposed to other on-line services. Audrey Gillan, *Race to Save New Victims of Child Porn*, The Guardian, Nov. 4, 2003, *available at* http://www.guardian.co.uk/child/story/0,7369,1077260,00.html (last visited Jan. 21, 2005).

Other types of criminals are similarly attracted to file-sharing networks. Unlike Napster, which was limited audio files, the new file-sharing programs allow users to download any type of file from other computers connected to the network. *Privacy and Security Risks* at 1. This feature creates unique privacy and security risks, because file-sharing programs potentially make every file on a computer available to millions of other users on the network. In fact, many users of file-sharing programs inadvertently make highly personal information available to other users. *Id.* at 1, 5-9. Congressional committee investigators "found that file-sharing programs could be used to easily obtain tax returns, medical records, attorney-client communications, and personal correspondence" from peer-to-peer users.[6] *Id.*

Continue to Climb, Information Week, Jan. 11, 2005, *available at* http://www.infomrationweek.com/story/showArticle.jhtml?articleID=57700595 (last visited Jan. 21, 2005).

[6] A search of one peer-to-peer network found at least 2,500 Microsoft Money backup files, which store the user's personal financial records, available for download. *Privacy and Security Risks* at 1.

High-tech vandals also exploit peer-to-peer networks to release computer viruses, worms, and other malicious computer files, often masking their handiwork as popular music files. *Privacy and Security Risks* at 11 (quoting Dr. John Hale, Director of the Center for Information Security at the University of Tulsa). Computer experts warn that the risks of viruses induced by security vulnerabilities in peer-to-peer software make using such software much more dangerous than merely surfing the Internet. *Id.* at 5. First, peer-to-peer networks put users' computers at high risk for viruses and other malicious files due to increased connectivity, flaws in software design, and potential for quick distribution of malicious programs. *Id*. Second, peer-to-peer networks offer little in the way of protection, leading one expert in computer security to state "banning [peer-to-peer] systems is definitely part of any reasonable best-practices approach to network security." *Id*. at 11-12.

Respondents engineered anonymous, decentralized, unsupervised, and unfiltered networks to create the fiction of ignorance of, and inability to control, illegal activity. The Ninth Circuit blessed these networks that make it increasingly difficult for law enforcement to detect distribution of child pornography and other illegal activity.

> Peer-to-peer programs have made it more difficult to identify the users. In the past [NCMEC was] able to easily identify offenders trading child pornography using peer-to-peer programs because their Internet Protocol (IP) addresses were visible and they were required to reveal their email addresses. This is no longer the case. When [NCMEC] receive[s] reports . . . , it is almost impossible to identify the perpetrators responsible for trading the illegal files. The anonymity of recent peer-to-peer technology has allowed individuals who exploit

> children to trade images and movies featuring the sexual assault of children with very little fear of detection.

Online Pornography: Closing the Doors on Pervasive Smut, Hearing Before House Subcommittee on Commerce, Trade, and Consumer Protection, 108th Cong. (May 6, 2004) (statement of Ernie Allen, President and Chief Executive Officer, National Center for Missing and Exploited Children).

Because the average user does not know whence she downloaded a file, she cannot give law enforcement any substantial information to track the offender. *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues*, Hearing Before the Federal Trade Commission, at 86 (Dec. 15, 2004) (statement of Michelle Collins, Director of the Exploited Child Unit of the National Center for Missing and Exploited Children), *available at* http://ftc.gov/bcp/workshops/filesharing/transcript_041215.pdf (last visited Jan. 21, 2005). Once the users disable their connection, law enforcement can do nothing to track down the offenders. *Id.*

II. THE LAW CONSISTENTLY HOLDS PARTIES LIABLE WHEN THEY FACILITATE THE ILLEGAL ACTIONS OF OTHERS.

The decision below is an anomaly among traditional principles of secondary liability in copyright law. Courts have consistently allocated responsibility for copyright infringement to those who have an ongoing relationship with the direct infringer. *See Sony*, 464 U.S. at 437. Respondents have the ability to update their software and otherwise maintain contact with their customers: facts that make their relationship with their users akin to that of a service provider who has an ongoing relationship with its customers. The Ninth Circuit ignored these facts and created a false analogy to a manufacturer that sells a product and loses all control over its use. *See Grokster II*, 380 F.3d at 1154. Respondents,

however, unlike Sony, are not limited in filtering infringing use by any technological or practical barrier, but by conscious choice.

These concepts of copyright secondary liability the Ninth Circuit ignores simply reflect general concepts of secondary liability from other areas of law, such as property, tort, criminal, and corporate law. The law has consistently taken a dim view of owners who fail to end illegal use of their property, or to take actions which increase the likelihood of illegal activity taking place. Respondents did not merely abdicate their responsibility to prevent illegal activity, but took affirmative action by facilitating illegal acts on their networks, and benefited from those illegal acts. Holding Respondents responsible for the illegal use of their networks is no different than ensuring that a landowner does not allow tenants to illegally use property and holding a store owner responsible for maintaining a safe workplace.

A. The Decision Below is an Anomaly Among Traditional Principles of Copyright Law.

Through the doctrine of secondary liability, courts recognize that it is improper to build a business based on the infringement of others' copyrights.[7] *Sony*, 464 U.S. at 438

[7] The Copyright Act defines an infringer as "anyone who violates any of the exclusive rights of the copyright owner . . . ." 17 U.S.C. § 501(a) (2004). Courts have not limited this definition to direct infringers, but imposed secondary liability to those who have some degree of involvement in the infringement. *Sony*, 464 U.S. at 434-35. Although the Act does not expressly mention secondary liability, Congress acknowledged its existence in the Act's legislative history. H.R. Rep. No. 1476, 94th Cong., 2d Sess. at 61, 159-60 (1976). Similarly, the *Digital Millennium Copyright Act* did not abolish secondary liability. *Aimster*, 334 F.3d at 655; *see also* 17 U.S.C. § 512. Although the Act gives Internet service providers safe harbor from liability in some cases, the service providers "must do what [they] can reasonably be asked to do to prevent the use of its service by 'repeat infringers.'" *Aimster*, 334 F.3d at 655 (citing 17 U.S.C. § 512 (i)(1)(A)).

n.18 (quoting *Shapiro, Bernstein & Co. v. H. L. Green Co.*, 316 F.2d 304, 308 (2d Cir. 1963)). This liability extends beyond those who actually manufacture or sell infringing material, and can apply to conduct that assists others in infringement. *Fonovisa, Inc.*, 76 F.3d at 259, 261.

In applying secondary liability to copyright law, courts have attempted to allocate responsibility for infringement where it may be most effectively exercised. *Sony*, 464 U.S. at 438 n.18; *Shapiro*, 316 F.2d at 307; *Gershwin Publ'g Corp.* v. *Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971). The ubiquitous example of this allocation of responsibility in copyright is that of the dance hall cases. The common facts of these cases involve a dance hall owner who hires a band that plays copyrighted music without authorization. *Aimster*, 334 F.3d at 654. The owners have contact with the bands, which are otherwise transient and difficult for the copyright holders to locate. Thus, courts reasoned it is the capability to contact and interact with the potential infringer that imposes responsibility to supervise their conduct. *See id.*; *Sony*, 464 U.S. at 437 (citing *Kalem* v. *Harper Bros.*, 222 U.S. 55 (1911)); *Shapiro*, 316 F.2d at 307 (finding liability derives from "ability to supervise").

Respondents, like the dance hall owners before them, have a "continuing relation with [the potential infringers]" which imbues them with responsibility for their actions. *Aimster*, 334 F.3d at 648. Respondents concede that they send advertising to their members. *Grokster II*, 380 F.3d at 1166. It is technically possible to even upgrade the software on the users' computers. JA 228-29, 182-83, 279-286. They chose to dismantle log-in and registration requirements that would give them additional contact with their users. *Grokster II*, 380 F.3d at 1165.

This ability to reach out to customers and alter a product in their hands—whether exercised or not—justifies the imposition of liability. This is precisely the type of situation where

the application of secondary liability is particularly appropriate. *Sony*, 464 U.S. at 437. On similar facts to the instant case, the Seventh Circuit found the designers of a peer-to-peer network provide a service as well as a product. Such service providers have:

> [A] continuing relation with [their] customers and therefore should be able to prevent, or at least limit, their infringing copyright by monitoring their use of the service and terminating them when it is discovered that they are infringing.

Aimster, 334 F.3d at 648.

When the Ninth Circuit found that Respondents did not have the ability to supervise infringing conduct, it ignored the fact that it did so by choice, not from any technological constraints. *Grokster II*, 380 F.3d at 1163. The Court stated that "[g]iven the lack of a registration and log-in process . . . Grokster has no ability to actually terminate the file sharing functions" despite the fact that Respondents themselves disabled these features. *Id.* at 1165.

The Ninth Circuit ignored the difference between flexible peer-to-peer technology and static products such as video tape recorders ("VTR"). As the District Court in *Napster* recognized, once a VTR was sold, its producer could no longer follow up with how consumers employed it. *A&M Records, Inc.* v. *Napster, Inc.*, 114 F. Supp. 2d 896, 916-17 (N.D. Cal. 2000). "Limiting distribution of the [VTR] machine to a class of non-infringers was not a possibility." Jane C. Ginsburg, *Copyright Use and Excuse on the Internet*, 24 Colum. VLA J.L. & Arts 1, 37 (2003) (hereinafter Ginsburg); *see also Sony*, 464 U.S. at 437-38 (observing that manufacturer had no ongoing relationship after sale); *Universal City Studios, Inc.* v. *Sony Corp.*, 480 F. Supp. 429, 461-62 (C.D. Cal. 1979).

Sony thus presented an all-or-nothing choice: if the manufacturers were liable, then the product could not be sold, despite its capacity for non-infringing uses; if manufacturers were not liable, then the product could be sold, despite its capacity for infringing uses. Ginsburg at 37. Left with this all-or-nothing choice, the Court allowed the new technology to survive. *Id.*

Technological advancements since *Sony* have removed the barrier between seller and user of the product and require that Respondents take responsibility for the use of their network. Peer-to-peer's "online technology makes possible the confinement of the service to a class of non-infringers." *Id.* Respondents are prevented from doing so only by choice and not by any technological barrier. Thus, the all-or-nothing predicament has been removed. *Sony*, 464 U.S. at 438 n.18. *Sony* noted that secondary liability "places responsibility where it *can and should* be effectively exercised," not merely where Respondents desire to do so. *Id.* (emphasis added).

Respondents not only have the ability to identify their infringing users, they are the only ones who may practically do so. Courts have found that recovering from direct infringers frequently proves difficult or impossible. *See Dreamland Ball Room, Inc.* v. *Shapiro, Bernstein & Co.*, 36 F.2d 354 (2d Cir. 1929) (citing example of iterant orchestras); *Shapiro*, 316 F.2d at 307-308 (2d Cir. 1963) (citing cases); *Screen Gems-Columbia Music, Inc.* v. *Mark-Fi Records, Inc.*, 256 F. Supp. 399 (S.D.N.Y. 1966) (discussing "fly-by-night" record pirates). Therefore, the only effective relief was found from a party in a position to stop the infringement. *See Aimster*, 334 F.3d at 654; Alan O. Sykes, *The Economics of Vicarious Liability*, 93 Yale L.J. 1231, 1241-42, 1272 (1984); *see also Dawson Chem. Co.* v. *Rohm & Haas Co.*, 448 U.S. 176, 188 (1980) (noting a similar rationale for the doctrine of contributory infringement in patent law). The Ninth Circuit, however, denies Petitioners a remedy and leaves them with

the impractical option of suing "a multitude of individual infringers" whose identities are close to impossible to obtain. *Aimster*, 334 F.3d at 645.

Similarly, parents and others concerned about the illegal activity are also without adequate remedy. For those outside the network, pedophiles and child pornographers are as difficult to identify as the infringing users. *See Online Pornography: Closing the Doors on Pervasive Smut*, Hearing Before the House Subcommittee on Commerce, Trade, and Consumer Protection, 108th Cong. (May 6, 2004) (statement of Ernie Allen, President and Chief Executive Officer, National Center for Missing and Exploited Children). As gatekeepers to the network, Respondents are the ones most capable of interdicting this illegal conduct.

A proper application of the doctrine of secondary liability serves the interests of the copyright holders, as well as law enforcement. As the only ones who can effectively exercise responsibility, Respondents must do so. *See Sony*, 464 U.S. at 438 n.18. Increased diligence in this area may give child predators and other criminals pause before engaging in their illegal conduct. "Just as the [Internet service providers] are working to tighten [their] content and shield kids, so must the peer-to-peer systems take responsibility." *Online Pornography: Closing the Doors on Pervasive Smut*, Before the House Subcommittee on Commerce, Trade, and Consumer Protection, 108th Cong. (May 6, 2004) (statement of Penny Nance, President, Kids First Coalition).

B. Decision Below is an Anomaly Among Traditional Principles of Secondary Liability Generally

The Ninth Circuit's holding runs counter to the underpinnings of longstanding, accepted theories of secondary liability in areas of the law beyond copyright. As Justice Holmes noted almost one hundred years ago, the concept of

secondary liability in copyright is premised "on principles recognized in every part of the law." *Kalem*, 222 U.S. at 63. An examination of these principles shows that the law requires individuals to supervise the use of their property and prohibits them from reducing the level of security in the face of known dangers. These concepts are widely applicable and extend to diverse areas of the law, including both civil (*e.g.*, tort, property, and corporate law) and criminal law. Persons may not condone illegal acts on their property (through inaction) nor endorse it (through positive action that encourages or otherwise supports illegal acts).

General principles of property law provide seminal examples of secondary liability of property owners for the illegal use of their property. In *Grosfield* v. *United States*, 276 U.S. 494, 495-496 (1928), the Court enjoined a property owner against the use of his property for the illegal manufacture of liquor by his tenant. This Court rejected the landlord's efforts to disclaim responsibility for the illegal use of the property by the tenant, noting:

> [I]t is no answer to the suit to say that the owner did not participate in the criminal act of the tenant. That the tenant may have been ousted and the illegal use of the premises ended before the decree is not conclusive, if the evidence furnish reasonable ground for apprehending a repetition of such use.

Id. at 498. Thus, the owner bears first responsibility to end the illegal use of his property. Indeed, the language suggests that the landlord has the burden of preventing reasonably foreseen repetition of the illegal use of the property.

Basic principles of tort law, likewise, place responsibility upon the landowner to adequately supervise his property to prevent illegal acts by any persons. *See* Restatement (Second) of Torts § 302A (1965). For instance, a landowner may be held liable for failing to provide adequate security protection under circumstances in which criminal attacks

upon entrants are otherwise foreseeable.[8] In *Gerentine* v. *Coastal Security Sys.*, 529 So.2d 1191 (Fla. Dist. Ct. App. 1988), the Court upheld a complaint seeking damages for the death of a convenience store employee who was abducted from the defendant's store. *Id.* at 1192. Interpreting Florida law, the Court found that the defendant's actions in reducing security protection despite four previous robberies of the convenience store, together with his decision not to create and enforce any policy to deter or prevent robberies, permitted recovery. *Id.* at 1193. This previous history of prevalent crime is analogous to the dominant use of Respondents' networks for illegal acts. Just as the convenience store owner was held liable for not taking steps to ensure the safe, legal use of his property, Respondents should be similarly liable for not preventing illegal use of their network.

Courts also recognize that in certain cases—even where they are otherwise under no preexisting duty to prevent a

---

[8] *See* Restatement (Second) of Torts § 344 cmt. f (1965):

> Since the possessor is not an insurer of the visitor's safety, he is ordinarily under no duty to exercise any care until he knows or has reason to know that the acts of the third person are occurring, or are about to occur. He may, however, know or have reason to know, from past experience, that there is a likelihood of conduct on the part of third persons in general which is likely to endanger the safety of the visitor, even though he has no reason to expect it on the part of any particular individual. If the place or character of his business, or his past experience, is such that he should reasonably anticipate careless or criminal conduct on the part of third persons, either generally or at some particular time, he may be under a duty to take precautions against it, and to provide a reasonably sufficient number of servants to afford a reasonable protection.

See also Stalzer v. *European Am. Bank*, 448 N.Y.S.2d 631, 635 (Civ. Ct. 1982) (finding that since the plaintiff was robbed while inside the defendant's bank, the defendant's knowledge of prior similar criminal activity imposed an obligation to "take all necessary protective measures and to provide a reasonably sufficient number of servants to afford security protection").

harmful act by some third party—an individual may still be liable for a failure to respond to illegal activity. In *Doe* v. *Walker*, 193 F.3d 42 (1st Cir. 1999), the plaintiff, a social guest invited to the defendant's home, was raped by three male guests of the defendant. *Id*. at 45-46 (applying Massachusetts law). The Court opined that if a social host becomes aware of criminal conduct being committed by one of his guests against another guest, and does nothing to avert or otherwise ameliorate the danger at no risk to himself, this failure to act could justify criminal charges against the host. *Id*. Even assuming, *arguendo*, Respondents have no other pre-existing duty to prevent the use of their network for child pornography, Respondents have knowledge that 90 percent of the traffic on their network is being used for illegal infringement and have failed to avert this danger.[9]

In addition, criminal law teaches that concepts of secondary liability extend to persons who have positively acted to encourage or otherwise endorse the illegal action in order to impose sanctions upon all that are culpable. In *United States* v. *Jewell*, 532 F.2d 697 (9th Cir. 1976), the defendant agreed to drive a car back from Mexico for an individual he had met in a bar. *Id.* at 699 n.1. The defendant became aware of a secret compartment in the vehicle, but deliberately avoided obtaining actual knowledge of the 110 pounds of marijuana contained therein. *Id.* at 698-99. The Court upheld a jury instruction which stated that knowledge of the controlled substance in his vehicle could be derived "solely and entirely because of a conscious purpose on his part to avoid learning the truth." *Id.* at 698. The Ninth Circuit wrongly dismissed the concept that Respondents should not be able to escape liability by willfully blinding themselves to

[9] *See also Staples* v. *CBL & Assocs., Inc.*, 15 S.W.3d 83, 90 (Tenn. 2000) (Finding that liability was incurred where the plaintiff was abducted from a shopping mall after reporting suspicious activity of her abductor to store employees and they took no further action).

the infringement as "rhetoric." *Grokster II*, 380 F.3d at 1165. Just as Mr. Jewell's narrow definition of knowing was inconsistent with congressional intent to effectively deal with "with the growing menace of drug abuse in the United States," *Jewell*, 532 F.2d at 703, so does the Ninth Circuit's reasoning render secondary liability meaningless.

Corporate law uses a similar concept of secondary liability to prevent endorsement and support of illegal acts. Generally, a parent corporation is not liable for the acts of its subsidiaries. *United States* v. *Bestfoods*, 524 U.S. 51, 61 (1998). This Court, however, has recognized an exception to this canonical rule to encourage corporations to structure themselves to comport with the law. "[A]n equally fundamental principle of corporate law, applicable to the parent-subsidiary relationship . . . , [is] that the corporate veil may be pierced and the shareholder held liable for the corporation's conduct when, *inter alia*, the corporate form would otherwise be misused to accomplish certain wrongful purposes. . . ." *Id.* at 62. The parent corporation bears responsibility over the conduct of its subsidiary where the corporation—like Respondents' network—is constructed merely to evade the law. The very creation of the shell corporation to absolve the parent of liability is a positive act that breeds illegal behavior, and *Bestfoods* stands for the proposition that such a positive act endorsing illegal behavior incurs secondary liability.

Secondary liability extends to persons that both condone illegal activity on their property through their own non-action, and endorse it through positive steps that encourage or support the illegal activity. In the same way, Respondents took no steps to secure their network in the face of known dangers. In fact, Respondents turned a blind eye to this danger. They were well aware of, and benefited from, the high propensity of infringement present in such places. *See Aimster*, 334 F.3d at 645 (stating "[t]he [file] swappers are ignorant or more commonly disdainful of copyright and in

any event discount the likelihood of being sued or prosecuted"). The incidents of child pornography and other illegal activity on these networks are well-known and well-documented. *See* Remarks of Attorney General John Ashcroft, *Peer-to-Peer Announcement*, May 14, 2004, *available at* http://www.usdoj.gov/ag/speeches/2004/51404agwebp2p.htm (last visited Jan. 21, 2005). Yet, like the store owner in *Gerentine*, Respondents not only failed to secure their network, but instead took positive action to reduce security and disabled devices able to detect and stop such activity. Respondents' removal of previously existing security restrictions on the Grokster network, such as removing the central server and the log-in requirement, is no different than the *Gerentine* convenience store's reduction of security protection. Like the store owner, Respondents should not escape liability for their actions.

CONCLUSION

For the foregoing reasons, as well as those set forth in the Brief for Respondents, the decision below should be reversed.

Respectfully submitted,

VIET D. DINH
Counsel of Record
CHRISTOPHER D. THUMA
BRIAN A. BENCZKOWSKI
BANCROFT ASSOCIATES PLLC
2121 Bancroft Place, N.W.
Washington, D.C. 20008
(202) 234-0090

Counsel for Amici