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 AUDIBLE MAGIC CORPORATION, DIGIMARC CORPORATION AND GRACENOTE

IN SUPPORT OF NEITHER PARTY

BRUCE V. SPIVA*
TYCKO, ZAVAREEI & SPIVA LLP
2001 L STREET, N.W.
SUITE 808
WASHINGTON, D.C. 20036
(202) 973-0900 (tel.)
(202) 973-0950 (fax)
Counsel for Amici Curiae

Additional Counsel On Inside Cover

January 24, 2005 * Counsel of Record

JEREMY H. STERN
COLE, RAYWID &
BRAVERMAN, LLP
2381 ROSECRANS AVENUE
SUITE 110
EL SEGUNDO, CA 90245
(310) 643-7999 (TEL.)
(310) 643-7997 (FAX)

COUNSEL FOR AUDIBLE
MAGIC CORPORATION

DAVID MARGLIN
GENERAL COUNSEL
GRACENOTE
2000 POWELL STREET
SUITE 1380
EMERYVILLE, CA 94608

COUNSEL FOR GRACENOTE

WILLIAM Y. CONWELL
CHIEF PATENT COUNSEL
DIGIMARC CORPORATION
9405 S.W. GEMINI DRIVE
BEAVERTON, OR 97008
(503) 469-4621 (TEL.)
(503) 469-4777 (FAX)

COUNSEL FOR DIGIMARC
CORPORATION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

MISCELLANEOUS

INTERESTS OF *AMICI CURIAE*[1]

Amici are providers of digital management services and technology solutions that, among other things, assist businesses in monitoring and monetizing the distribution of electronic data, including digitized copyrighted content, as well as detecting and preventing the unauthorized distribution of such content.

Amicus Audible Magic Corporation ("Audible Magic") is a technology and services company founded in 1999 that provides content management and information services to the Internet, media and entertainment industries as well as to government agencies and academic institutions. Audible Magic's technology and services are based upon its patented media identification and classification technology, its media monitoring and management software and appliance, and its extensive reference database of digital fingerprints of copyrighted music and other digital content. Its digital fingerprinting and filtering technology is designed to monitor, track, manage, and in some cases filter copyrighted multimedia content in all of its forms, including radio and TV analog broadcasts, Internet and satellite streams, stored media files, as well as peer-to-peer ("P2P") and private network file transfers.

Amicus Digimarc Corporation ("Digimarc") provides, among other things, "digital watermarking" solutions and technology. Digital watermarking is a proven technology used by major TV broadcasters, movie studios, record labels,

---

[1] Counsel for the Petitioners and Respondents have consented to the filing of this brief. Their consent letters have been filed with the clerk of the Court. No counsel for a party in this Court authored this brief in whole or in part, and no person or entity, other than Audible Magic Corporation, Digimarc Corporation and Gracenote as *amici curiae,* made a monetary contribution to the preparation or submission of this brief.

stock photo agencies, and governments around the world. It has been deployed in billions of content objects, including audio, video, digital images and printed materials. Digital watermarking is widely used to track, monitor, and manage use of content as it is distributed. Management of content can include linking to additional system or network information and metadata (*e.g.* rights management information) as well as enforcement of usage rules in local devices. This technology allows its customers to track – and, as necessary, inhibit – the dissemination of "digitally watermarked" content.

Amicus Gracenote is the developer of MusicID technology, including an Internet-based service that recognizes and identifies digital audio recordings (by analyzing the data in the recording) and associates certain identifying "metadata" in the recording. Its music recognition service is widely used throughout the Internet, consumer electronics, and entertainment industries and is powered by CDDB, the largest online database of audio CD and song titles in the world. Its solutions have been applied to a myriad of online services, including Apple's iTunes Music Service.

Of particular relevance to *amici*, and of particular significance here, are the notions advanced by the Respondents – and accepted by the Ninth Circuit Court of Appeals – that (1) distributed P2P networks are incapable of integrating technological solutions that prevent unauthorized distribution and reproduction of copyrighted works, and (2) integration of amici's technology would lead to the doom of Respondents' P2P networks and online services generally. Amici are submitting this brief to make the Court aware of readily available technologies that can separate infringing and non-infringing content. These innovative technologies – which are deployed around the world today in various analogous commercial settings -- show that the protection of copy-

righted works and the development of technology and the marketplace for content can go hand-in-hand.

INTRODUCTION AND BACKGROUND

Amici file this brief in support of neither party in the case and further take no position on any of the legal issues in this case. Amici submit this brief to provide information to the Court about existing technologies that would in fact permit Respondents - despite the decentralized nature of their P2P file-trading networks - to identify and significantly diminish the copyright infringement they enable.

SUMMARY OF ARGUMENT

Today's marketplace already includes technological solutions for identifying and limiting the illegal dissemination of copyrighted works on P2P file-trading networks. This technology can work effectively whether such networks are fostered by centralized or decentralized servers. The failure of Respondents to utilize these existing technologies represents a *choice*, not a stricture inherent in their software design, as the Ninth Circuit suggested, *see id.* at 1163, or in the decentralized nature of their services. Integration of these technologies in Respondents' software and services will not curtail technological innovation or new markets for content distribution. To the contrary, it will facilitate the creation of legitimate commerce over P2P networks and permit the authorized distribution of copyrighted works while insuring that copyright owners are compensated for such copying. This in turn would create the proper economic incentives for the further development and technological innovation of P2P services. The end result would be a broader method of distribution for copyright owners, a larger potential market of online purchasers (as opposed to infringers), a safer distribution sys-

tem for consumers of content, and a more attractive and profitable marketplace for P2P network operators.

ARGUMENT

I. TODAY'S MARKETPLACE ALREADY INCLUDES TECHNOLOGICAL SOLUTIONS FOR IDENTIFYING AND LIMITING THE DISSEMINATION OF COPYRIGHTED WORKS IN P2P NETWORKS

The Ninth Circuit held that "'Plaintiffs' notices [to Defendants'] of infringing conduct are irrelevant,' because 'they arrive when Defendants do nothing to facilitate, and cannot do anything to stop, the alleged infringement' of specific copyrighted content." *Metro-Goldwyn-Mayer Studios, Inc., et al. v. Grokster Ltd, et al.*, 380 F.3d 1154, 1162 (9th Cir. 2004) (citations omitted). This is not so. There are available technologies (discussed in the record below) that P2P services can use to separate infringing and non-infringing works, and either facilitate rightful payment for or allow the blocking of the distribution and copying of copyrighted works over a decentralized P2P network. These technologies can protect the rights of copyright owners while also allowing non-infringing uses of P2P networks to continue. *See* Declaration of Prof. Leonard Kleinrock J.A. 241-86 (hereinafter "Kleinrock Decl."); Declaration of David Hyman J.A. 224-27 (hereinafter "Hyman Decl."); Declaration of Vance Ikezoye J.A. 228-32 (hereinafter "Ikezoye Decl.").

There are various aspects to inhibiting piracy of copyrighted works on a P2P system, including (1) identifying digital files correctly, (2) handling the files in an appropriate manner based on their identification, and (3) enabling illegitimate files to be forensically tracked to their source. There are many proven technologies available for each. *See* J.A.

279-86 (Kleinrock Decl.).

A. Digital Fingerprinting and Filtering

Existing digital fingerprinting and filtering technology, such as that offered by Amici Audible Magic and Gracenote, can prevent unauthorized recordings from being distributed on P2P file-trading systems like those operated by Respondents. J.A. 279-86 (Kleinrock Decl.) ; J.A. 228 (Ikezoye Decl.); J.A. 224 (Hyman Decl.). This technology has been available since the time that Respondents began operating.[2] J.A. 224 (Hyman Decl.).

Digital fingerprinting is an audio recognition technology. It provides a robust method of precisely identifying digital music and video soundtrack content, regardless of source or format (*e.g.*, MP3 download, WAV file, streaming audio signal, compact disc, DVD, or radio broadcast). The analysis performed by this technology produces a set of mathematical values called a "feature vector" or "digital fingerprint," which is unique to a particular master recording. In essence, each digital fingerprint identifies a master recording, much as a human fingerprint identifies a person, or a box score identifies a specific baseball game. *See* J.A. 230 (Ikezoye Decl.). The "fingerprints" are precise enough to differentiate between various live and studio performances of a single song. The fingerprints are also very small, which makes their use practical in blocking the distribution and copying of unauthorized recordings.

Amici maintain separate databases of fingerprints for mil-

[2] Moreover, filtering to block dissemination of copyrighted works is far more accurate (and, in many ways, far easier) than, for example, preventing the dissemination of all pornographic files through text-based filters. This is because filtering copyrighted works involves blocking specific works using digital characteristics rather than all files containing terms like "nudity."

lions of copyrighted songs, each representing almost all of the music available for purchase in North America. J.A. 231 (Ikezoye Decl.); J.A. 225 (Hyman Decl.). The fingerprints in these databases (or those of competing companies) could be used to evaluate songs that a user sought to distribute over the Internet.

Essentially, fingerprinting software could be integrated into the P2P user application or on a server operated by the P2P system operator such as Grokster or StreamCast. In either case, the fingerprinting technology would create a fingerprint of each digital recording that a user sought to distribute and transmit it over the Internet to a reference database. The unknown fingerprint would then be compared to the fingerprints in the reference database to determine whether the file is authorized for distribution.[3] Those that are not authorized for distribution would be blocked, while those files that are authorized for distribution could be distributed and copied. J.A. 279-85 (Kleinrock Decl.); J.A. 231-32 (Ikezoye Decl.); J.A. 225-27 (Hyman Decl.). It is important to point out that integration of digital fingerprinting and filtering technologies into P2P networks would, in and of itself, in no way interfere with the free flow of public domain works, or even copyrighted works that the authors wanted to distribute freely over the Internet.

---

[3] Fingerprinting and filtering technology can be designed either as "filter-in" or "filter-out" systems. A "filter-in" system includes in the reference database only fingerprints of those recordings that the copyright holders have authorized for distribution. If the fingerprint of the unknown audio file matches a fingerprint in the reference database, the user would be permitted to distribute and copy the audio file. In contrast, a "filter-out" system includes in the reference database only fingerprints of those recordings that are not authorized for distribution, and a match would prevent distribution, while no match would permit distribution. J.A. 279-85 (Kleinrock Decl.); J.A. 232 (Ikezoye Decl.); J.A. 226-27 (Hyman Decl.).

Working with their respective licensees, both Gracenote and Audible Magic have experience in testing the integration of fingerprinting and filtering technology in peer-to-peer environments over the Internet. The technical impediments faced during these tests have been overcome. Based on this experience, and the experience of licensees in using these enabling technologies, the question is not whether the deployment of such technologies would work in commercial P2P services (including those with decentralized architectures), but rather whether P2P operators will choose to incorporate them.

In addition, Audible Magic's technology has been deployed and proven in other settings to assist entities such as performing rights organizations (PROs), Internet Service Providers ("ISPs"), digital content owners, advertising and public relations agencies, as well as educational institutions. J.A. 228-29 (Ikezoye Decl.). For example, Audible Magic's CopySense appliance has been deployed by ISP networks and university and college networks to monitor and manage precious bandwidth which increasingly is being consumed by illegal P2P file sharing. Another service of the company enables CD replicators to identify the tracks that they are reproducing for CD distribution to ensure that the distributor has the proper licenses from content owners to reproduce and distribute the content. Other applications include assisting PROs with real-time radio broadcasting monitoring to allow accurate collection and distribution of copyright royalties, and collecting comprehensive data for advertising and PR agencies on the number of occurrences of a particular advertisement on a station that has contracted to transmit it. All of these services are made possible by Audible Magic's digital fingerprinting and filtering technology.

Similarly, leading software and hardware developers, such as AOL/Winamp, Apple, Kenwood, Pioneer, RealNetworks,

and Creative Labs, currently use Gracenote's technology in their applications and products to identify music being played. The technology time and again has proven effective in mass consumer environments. Gracenote too has developed technology that can be adapted to create a filtering service for a P2P system. In fact, Gracenote offered its services to Music City, a predecessor company to Respondent StreamCast, but StreamCast declined. J.A. 225 (Hyman Decl.).

B. Digital Watermarking

In addition, digital watermarking can be used in several ways to inhibit the unauthorized distribution of copyrighted content. Digital watermarking is the science of hiding extra information, such as identification or control signals, in media content. For example, the digital "pixels" making up a movie can be slightly altered in value to represent extra information, while not visibly impairing the appearance of the movie to human viewers.

The extra information represented by digital watermarks travels with the content, persisting through changes in file format, and through transformation between digital and analog form. One application of digital watermarking is to indelibly mark electronic media content delivered to a recipient with a serial number by which transaction information (*e.g.* purchase date, recipient, and vendor) can be determined.

Such digital watermarking is widely used by major movie studios and music companies who send "pre-release" copies of upcoming movies and CDs to global manufacturing facilities, reviewers, and other marketing resources. The recipient-identification provided by watermark data has allowed

unauthorized content found on P2P networks to be traced back to the person receiving the source pre-release copy.[4]

Digital watermarking and fingerprinting can also be employed jointly. For example, a file could be checked for a watermark to determine appropriate treatment. If no digital watermark is found, a fingerprint could be computed to identify the file. Once the file's identity is known, an appropriate treatment policy could be determined (*e.g.* by reference to the CDDB or Audible Magic databases), and a watermark could be embedded so that this information thereafter travels with the file.

Current watermarks are robust against attack. Attempts to impair the watermark require impairing the host content, *e.g.*, making a movie blurry, or a song noisy. Moreover, such tampering with a copyright protection measure can trigger liability under the Digital Millennium Copyright Act.[5]

All of these arrangements address the legitimate concerns of the copyright holders, while balancing the corresponding public interest in continued use of P2P file-trading services to share public domain and freely-copyable works. All of these arrangements are well suited for service in P2P environments like those used by Respondents – whether with centralized or

---

[4] *See, e.g., Actor Must Pay Studios For Sharing Film Copies; The $600,000 Penalty Might Deter Others From Passing Along 'Screeners' During Awards Season*, Los Angeles Times, Nov. 24, 2004, at C1; and *Labels' Top Priority: Leak Prevention*, Los Angeles Times, Oct. 13, 2002, at E46 ("Advance copies of Faith Hill's new "Cry" album sent by Warner Bros. Records to journalists, retailers and radio programmers included a 'watermark' encoded into the disc that identifies each person a copy was sent to." "Warner Bros. sources confirm that they have identified the source of the Hill leak and that legal action for copyright violation is being considered against a journalist.")

[5] *See* e.*g.*, 17 U.S.C. § 1202(b).

decentralized servers. *None* of these arrangements to prevent inappropriate copying or redistribution, however, can succeed, unless Respondents do their part.

II. INTEGRATION OF TECHNOLOGY SUCH AS AMICI'S WOULD NOT CURTAIL TECHNOLOGICAL OR SERVICE INNOVATION.

Far from stymieing the creation of new markets and technological innovation, as the Ninth Circuit suggested, protection of copyrighted works from the massive piracy occurring on Respondents' P2P networks will actually foster innovative technologies that permit greater and safer dissemination of authorized works while at the same time insuring due compensation to copyright owners. Innovative technologies, such as those described above, will not continue to develop as quickly if the copyrighted works they seek to protect are readily available for free on the P2P networks, and there is no incentive for Respondents to curtail the infringement that they enable.

A legitimate P2P content distribution system would create significant benefits for users, copyright holders and P2P companies, and all others who would benefit from the resulting legitimate commercial markets. The users of the system would get one-stop shopping for media content from trusted vendors. Users of such a P2P network could simultaneously lessen the threat posed by the unpleasant surprises that are rampant under the systems spawned by Respondents – including null files, viruses, Trojan-horses masquerading as movies, pornography mislabled with an innocuous file name – while gaining confidence that they are not infringing copyrights. Copyright holders would gain from a legitimized P2P content distribution channel that would satisfy their customers. And responsible P2P file-trading system operators would obtain a reasonable return on investment for distributing content legally. But none of these emerging technologies

can ever take root in the commercial market against the competition of "Everything for Free" posed by current operation of Respondents' existing services.

CONCLUSION

Amici do not advocate for a decision in favor of either party. Instead, they are filing this Amici Curiae to inform the Court of the robust and viable range of technological options that are readily deployable in the context of Respondents' P2P networks. Once such technological solutions are integrated into P2P platforms, a legitimate market for file sharing of digital content can develop and flourish, bringing more consumers access to more content, increased compensation to rights holders and greater incentives for Respondents and other P2P networks to compete and innovate in a myriad of ways.

Respectfully submitted,

BRUCE V. SPIVA*
TYCKO, ZAVAREEI & SPIVA LLP
2001 L STREET, NW SUITE 808
WASHINGTON, DC 20036

*Counsel of Record

OF COUNSEL:

JEREMY H. STERN
COLE, RAYWID & BRAVERMAN, LLP
2381 ROSECRANS AVENUE
SUITE 110
EL SEGUNDO, CA 90245
(310) 643-7999 (TEL.)
(310) 643-7997 (FAX)

COUNSEL FOR AUDIBLE MAGIC CORPORATION

DAVID MARGLIN
GENERAL COUNSEL
GRACENOTE
2000 POWELL STREET
SUITE 1380
EMERYVILLE, CA 94608

COUNSEL FOR GRACENOTE

WILLIAM Y. CONWELL
CHIEF PATENT COUNSEL
DIGIMARC CORPORATION
9405 S.W. GEMINI DRIVE
BEAVERTON, OR 97008
(503) 469-4621 (TEL.)
(503) 469-4777 (FAX)

COUNSEL FOR DIGIMARC
CORPORATION