

# New York Law Journal



Web address: <http://www.nylj.com>

VOLUME 232—NO. 8

TUESDAY, JULY 13, 2004

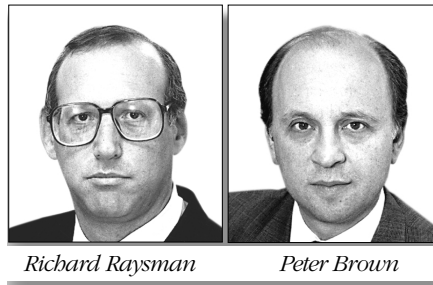
## COMPUTER LAW

BY RICHARD RAYSMAN AND PETER BROWN

### *Copyright and File-Sharing: Identifying Anonymous Defendants*

Peer-to-peer (P2P) technology facilitates direct online communications between two or more computers, allowing users to perform various functions such as sending instant messages and transferring files. Several software vendors have capitalized on P2P by creating networks that enable users to search each other's computers for desired files and to transfer such files directly from one computer to another, despite the fact that these users would otherwise have no connection with, or knowledge of, each other. Since their inception with Napster in 1999, P2P search engines have facilitated billions of file transfers by millions of anonymous Internet users.<sup>1</sup> The easy, direct transferability of higher-quality digital copies of copyrighted works — such as music, movies, and software — has presented a serious challenge to copyright owners seeking to protect their works from unauthorized copying and distribution.

While it is feasible to determine a user's Internet Protocol — a unique numerical identifier assigned to every computer that accesses the Internet — as well as the time at which a user connected to a P2P



Richard Raysman

Peter Brown

network, it is extraordinarily difficult to derive personally identifiable information from Internet Protocol-plus-timestamp information without the assistance of an Internet Service Provider (ISP).

The original P2P search engine, Napster, was based on a model that provided search results on centralized servers. P2P has since evolved into a decentralized world that eliminates infringing material from any central server. In the past, rights holders have successfully sought to enjoin centralized file-sharing networks from engaging in vicarious and contributory copyright infringement, but that tactic is becoming less effective as P2P entities have decentralized and altered their business practices to avoid further liability.<sup>2</sup> At present, copyright owners increasingly are seeking to hold Internet file traders liable for direct infringement, despite the difficulty of identifying anonymous defendants.

#### Subpoenas & Fallout

Copyright owners have sought to utilize the subpoena provisions of the Digital Millennium Copyright Act, §512(h),<sup>3</sup> to

identify anonymous users of file-sharing networks. In *RIAA v. Verizon*, 351 F3d 1229 (DC Cir 2003), the Court of Appeals held that §512(h) does not authorize the issuance of a subpoena to an ISP that transmits infringing materials but does not store any such material on its servers. The Recording Industry Association of America or RIAA, had previously used the subpoena provisions of the Digital Millennium Copyright Act to compel ISPs to reveal the names of subscribers suspected of sharing and trading copyrighted music files over P2P networks. However, Verizon successfully argued that §512(h), by its terms, precluded the issuance of a subpoena to an ISP that merely acted as a conduit for P2P communications, as the ISP can neither “remove” nor “disable access to” infringing material that is not stored on its servers.<sup>4</sup>

Although not unsympathetic to the widespread copyright infringement at issue in *RIAA v. Verizon*, the court stated that P2P file-sharing was unforeseeable to Congress when drafting the Digital Millennium Copyright Act and, in turn, reasoned that §512(h) was not formulated broadly enough to reach the new technology.<sup>5</sup>

Not surprisingly, congressional hearings regarding illegitimate uses of P2P file-sharing networks began one week after arguments commenced in *RIAA v. Verizon*. Nine senators commented and eleven witnesses testified on both sides of the issue in an effort to determine what, if any, action should be taken by the Congress to ameliorate the negative impact of P2P

**Richard Raysman** and **Peter Brown** are partners at Brown Raysman Millstein Felder & Steiner. They are co-authors of “Computer Law: Drafting and Negotiating Forms and Agreements” (Law Journal Press, [lawcatalog.com](http://lawcatalog.com)). **Andrew S. Chalson**, a summer associate at the firm, assisted in the preparation of this article.

file-sharing on the entertainment industry.<sup>6</sup> In May 2004, the General Accounting Office issued a report to requesting members of congress regarding P2P file-sharing, promising that the Justice Department's recently created Intellectual Property Task Force will examine how the department handles intellectual property rights violations and recommend legislative changes, if needed.<sup>7</sup>

### John Does, Severance and Discovery

Although the D.C. Circuit's decision in *RIAA v. Verizon* is not binding on other Federal Courts of Appeals, rights holders have seemingly chosen to forego filing Digital Millennium Copyright Act subpoenas in additional jurisdictions in favor of bringing single actions against multiple John Does. In filing such John Doe suits without mention of the act, copyright owners have taken a different procedural tack in attempting to obtain the identity of anonymous infringers. In at least fourteen cases since January 2004, the music industry has simultaneously filed complaints against numerous John Does, motions for leave to take immediate discovery, and declarations in support of the immediate discovery motions. Proposed orders granting the motions for immediate discovery were occasionally included in these filings.<sup>8</sup>

In response to music industry filings, several courts have ordered that the industry's John Doe cases, seeking permissive joinder of anonymous defendants, must be severed because the injuries alleged by rights holders do not result from the "same transaction or occurrence" as mandated by Federal Rule of Civil Procedure 20.<sup>9</sup> Anonymous defendants have argued that their interactions with various plaintiffs fail to conform to the standards of Rule 20 because there is no evidence that the joined defendants downloaded any copyrighted materials from one another, as opposed to any other users of P2P networks.

Defendants have further noted that if they are connected, it is only by their use of the same ISP.<sup>10</sup> These facts, taken together, make it easier for the plaintiffs to file for and obtain discovery, but, as the district court noted in *Bridgeport Music, Inc. v. 11C Music*, 202 FRD. 229, 231 (M.D. Tenn. 2001), they serve to bury defendants' lawyers in "an overwhelming onslaught of materials and information unrelated to the specific claims against each defendant." Several judges have seemingly agreed with defendants' rationale in issuing the aforementioned severance orders.<sup>11</sup>

Notwithstanding the initial delay due to required severances, rights holders may be able to make a strong argument to support their motions for immediate discovery. By providing ISPs with unique Internet Protocols, along with specific dates and times of infringing activities, rights holders should be able to avoid accusations of overly burdensome electronic discovery requests. When provided with Internet Protocol-plus-timestamp information, an ISP often can quickly and easily identify the infringing computer, and in turn the name and address of that computer's subscriber. Furthermore, ISPs do not keep logs of Internet Protocol assignments indefinitely, so immediate discovery requests may therefore be appropriate to make sure that identifying information is procured before it is no longer available. In fact, at least one court, after ordering severance of several hundred anonymous defendants, granted a rights holder's motion for expedited discovery with respect to a single defendant. The court's order granting discovery stated that the defendant's ISP was officially on notice that it possessed and should preserve information related to litigation.<sup>12</sup> In light of this order and the ephemeral nature of Internet Protocol logging, ISPs should consider producing, disseminating and enforcing strict document retention/ destruction policies in order to

avoid allegations of bad faith during discovery proceedings.

### Protection of Anonymity

Assuming that rights holders choose to sever and refile and that discovery requests are not deemed overly burdensome, judges may be faced with the First Amendment issue that was raised at the District Court for the District of Columbia in *RIAA v. Verizon*, but not addressed by the Court of Appeals: whether a copyright holder's right to protect its intellectual property in a judicial proceeding outweighs an Internet user's right to engage in anonymous speech.

The Supreme Court has recognized that the First Amendment protects speech on the Internet, see *Reno v. ACLU*, 521 US 844, 870 (1997) (finding no basis for qualifying the level of First Amendment scrutiny applied to the Internet), as well as a First Amendment right to engage in anonymous speech, see *McIntyre v. Ohio Electronics Commission*, 514 US 334 (1995). However, the Court also has noted that there are limitations on the right to free speech, such as the application of defamation laws, and several lower courts have created multi-part balancing tests aimed at determining whether a plaintiff's need outweighs a defendant's First Amendment rights.

In *Doe v. 2TheMart.com, Inc.*, 140 FSupp 2d 1088, 1095 (W.D. Wash. 2001), the district court enunciated a four-part balancing test in which a court must determine (1) whether a Federal Rules of Civil Procedure 45 civil subpoena is "issued in good faith;" (2) whether the information that the party seeks "relates to a core claim or defense;" (3) whether the information identifying the defendant "is directly and materially relevant to that claim or defense;" and (4) whether the information sought is available from any other source. If these factors balance in the defendant's favor, a civil subpoena is

unlikely to be honored, and accusations of bad faith could be made against the plaintiff.

In 2001, the New Jersey Appellate Division appended the duties imposed by *2TheMart.com* on plaintiffs seeking to identify anonymous defendants. In *Dendrite International, Inc. v. Doe*, 342 NJ Super 134, 141 (App Div 2001), the court set forth a balancing test that incorporated the *2TheMart.com* factors, while further requiring plaintiffs to "undertake efforts to notify" the defendant that discovery is being sought, and to provide a "reasonable opportunity" to oppose the request. The *Dendrite* court went on to state that a plaintiff must essentially set forth a prima facie case against an anonymous defendant while presenting sufficient evidence to support each cause of action pleaded.

In the music industry's recent barrage of John Doe suits, it is clear from the pleadings that sufficient evidence of copyright infringement exists in at least a handful of cases. It is also clear that only an ISP can match names and addresses to timestamped Internet Protocols. However, judges have yet to weigh in on the First Amendment balancing issue in P2P cases, and are unlikely to do so until rights holders file individual discovery motions in response to severance orders.<sup>13</sup>

An alternative means of identifying an anonymous defendant would be to utilize the criminal provisions associated with the Federal Copyright Act<sup>14</sup> by turning over evidence of infringement to federal prosecutors in the hope that they would accept a case and issue a grand jury subpoena aimed at revealing an anonymous infringer, at which time a subsequent civil suit could be filed.<sup>15</sup> However, prosecutors are unlikely at this time to take cases that involve anything less than large-scale distribution of copyrighted works (for reasons ranging from limited economic and personnel resources to practical concerns such as deterrence),

and rights holders have been targeting John Does whose violations run the gamut of egregiousness, from a handful of infringements to thousands. At present, many rights holders view criminal sanctions as an extreme measure, but if judges in civil John Doe cases continuously rule in favor of defendants, grand jury subpoenas may represent the only recourse for aggrieved parties.

## Conclusion

As file-sharing technology evolves, so too do the procedures fashioned by rights holders to prevent the anonymous copyright infringement that is running rampant on the Internet. Many infringers lack a full understanding of the illegality and serious consequences of their actions, and rights holders are actively seeking an effective deterrent. Identifying anonymous infringers in the pursuit of civil damages is the first major step towards such deterrence. The music industry in particular has been navigating the labyrinth of anonymous discovery, and appears to be approaching the last few hurdles that separate it from the discovery motions that it seeks. In the fast-paced world of digital piracy and P2P file-sharing in particular, attorneys for rights holders must now focus on the specificity of their discovery requests and the accumulation of prima facie evidence of infringement in order to streamline and simplify a judge's review of anonymous discovery motions.

1. Recent Congressional testimony cited over 2.6 billion P2P downloads per month. See Privacy and Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Permanent Subcomm. on Inv. of the Senate Comm. on Gov. Affairs, 108th Cong. (Sept. 30, 2003) (hereinafter "Privacy and Piracy"). As of May 27, 2003, at least one popular P2P network ("Kazaa") had been downloaded over 229 million times. See John Borland, File Swapping Shifts Up a Gear, CNET News.com at [http://www.news.com/2100-1026\\_3-1009742.html](http://www.news.com/2100-1026_3-1009742.html), last visited June 9, 2004.

2. See *A&M Records, Inc. v. Napster*, 293 F3d 1004 (9th Cir.2001) (finding Napster guilty of vicarious and contributory infringement); Cf. *Metro-*

*Goldwyn-Mayer Studios, Inc. v. Grokster, Inc.*, 259 F Supp 2d 1029 (C.D. Cal. 2003), appeal docketed, No. 03-56236 (9th Cir 2004) (finding Grokster not guilty of vicarious and contributory infringement). Legislation that threatens to outlaw P2P networks altogether was proposed in light of the *Grokster* decision. See Declan McCullagh, Senate Bill Bans P2P Networks, CNET News.com at [http://news.com.com/Senate+bill+bans+P2P+networks/2100-1027\\_3-5244796.html?tag=st-rc.targ\\_mb](http://news.com.com/Senate+bill+bans+P2P+networks/2100-1027_3-5244796.html?tag=st-rc.targ_mb), last visited June 28, 2004.

3. DMCA §512(h) reads, in relevant part, "A copyright owner ...may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection." 17 USC §512(h)(1).

4. See generally 17 USC §512(c)(3)(A).

5. *Recording Industry Assoc of America, Inc. v. Verizon Internet Services, Inc.*, 351 F3d 1229, 1238 (D.C. Cir. 2003) (as amended).

6. See Privacy and Piracy, supra at n.1.

7. File Sharing: Selected Universities Report Taking Action to Reduce Copyright Infringement, United States General Accounting Office Report to Congressional Requesters, GAO-04-503 (May 2004) at <http://www.gao.gov/new.items/d04503.pdf>, last visited June 28, 2004.

8. See *RIAA v. The People* at [http://www.eff.org/INTERNET\\_PROTOCOL/P2P-riaa-v-thepeople.php](http://www.eff.org/INTERNET_PROTOCOL/P2P-riaa-v-thepeople.php), last visited June 28, 2004.

9. See, e.g., *BMG Music v. Does 1-203*, No. 04-650 (E.D. Pa. March 5, 2004); *Interscope Records v. Does 1-25*, No. 6:04-cv-197-Orl-22DAB (M.D. Fla April 1, 2004).

10. See, e.g., *Motown Record Company, et al. v. Does 1-252: Motion to Quash from Defendant Doe #106*, No. 04-cv-0439 (N.D. Ga. April 12, 2004).

11. See, e.g., *BMG Music v. Does 1-203: Order Requiring Severance*, No. 04-650 (E.D. Pa. March 5, 2004); *Interscope Records v. Does 1-25: Order Requiring Severance*, No. 6:04-cv-197-Orl-22DAB (April 29, 2004).

12. See *BMG Music v. Does 1-203: Order Granting Motion for Immediate Discovery with Respect to Defendant Doe #1*, No. 04-650 (E.D. Pa. March 5, 2004).

13. Interestingly, at the time of this writing the discovery order in *BMG v. Does*, supra at n.12, involved no consideration of First Amendment issues.

14. See generally 17 USC. §506 (criminal offenses), 18 USC §§2318 (trafficking in ...copies of ...audiovisual works) & 2319 (criminal infringement of a copyright); see also David McGuire, Lawmakers Push Prison for Online Pirates, *WashingtonPost.com*, March 31, 2004, at <http://www.washingtonpost.com/ac2/wp-dyn/A40145-2004Mar31>, last visited June 9, 2004 (noting that a Congressional panel recently approved the "Piracy Deterrence and Education Act of 2004," which if signed into law would expose, inter alios, individuals who traded more than 1,000 songs on P2P networks to up to three years of jail time).

15. Indeed, the U.S. Senate has recently overwhelmingly approved a proposal that would let federal prosecutors file civil lawsuits against suspected copyright infringers. See Declan McCullagh, Senate Oks Antipiracy Plan, CNET News.com at [http://www.news.com/2100-1027\\_3-5248333.html](http://www.news.com/2100-1027_3-5248333.html), last visited June 28, 2004.