

# New York Law Journal

## Technology Today

Tuesday, June 8, 2004

### 'Doe' Defendants

*The RIAA's New Front in the Battle Against 'P2P' Filesharers*

The Digital Millennium Copyright Act (17 U.S.C. §512), enacted in 1998, contains certain "safe harbor" provisions that, under specified circumstances, protect an Internet service provider (ISP) from liability for activities of users.

As a counterpoint to these protections, §512(h) gave copyright owners the right to subpoena ISPs to determine the identity of individuals allegedly responsible for infringing activities. No action in court is necessary under §512(h).

In *Recording Industry Association of America v. Verizon Internet Servs.*, 351 F.3d 1229 (2003), the U.S. Court of Appeals for the D.C. Circuit invalidated the use of the §512(h) subpoenas as applied against ISP customers engaging in "file-sharing" of copyrighted works on peer-to-peer (P2P) networks like Napster, KaaZaa, and Grokster.

Though the court was sympathetic to the plight of the music industry — represented by the Recording Industry Association of America (RIAA) in that case — it felt limited by the language of the statute, which was written at a time when file-sharing on P2P networks had not been foreseen:

We are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights. It is not the province of the courts, however, to rewrite the Digital Millennium Copyright Act to make it fit a new and unforeseen Internet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and

**Peter J. Pizzi** is a partner in Connell Foley and chairman of the Internet and information law practice group. **M. Trevor Lyons**, an associate at the firm, assisted in the preparation of this article.

#### INTERNET ISSUES



**PETER J. PIZZI**

software industries.

In response to the *Verizon* decision, the RIAA has turned to the use of "John/Jane Doe" lawsuits as the mechanism by which to identify file-sharing customers of ISPs and obtain judicial relief against copyright infringement. Since January, and continuing through the end of last month, the RIAA has filed hundreds of lawsuits against "Doe" defendants in federal district courts around the country.

In these cases, the RIAA<sup>1</sup> usually files a complaint and then immediately applies for issuance of a subpoena directed to the Doe defendant's ISP, seeking to compel production by the ISP of account information identifying the Doe defendants. Because the Federal Rules of Civil Procedure are largely silent concerning pre-answer ex parte discovery, these applications pose novel procedural and notice issues.

In these recent Doe suits, the RIAA alleges that heavy file-sharing activity can be traced to

specific Internet protocol (IP) addresses assigned to individual customers of various ISPs around the country. IP addresses are unique to every computer connected to the Internet. The RIAA apparently uses "packet sniffer" software to trace file-sharing activity to particular IP addresses. From the IP address, the RIAA can determine the ISP serving the customer represented by the IP address. The goal of the subpoenas is to match IP data of the file-sharers with an ISP account name and residence address.

The RIAA motion papers stress the need for the issuance of an immediate subpoena to the ISP because of the practice of ISPs to erase IP information periodically. ISPs using "dynamic" IP systems assign a new IP address to each customer each time the customer connects to the Internet. Because of the voluminous nature of such accumulated IP data, ISPs using dynamic IP systems do not retain historic IP data for more than a few weeks.

Even where a file-sharer is assigned a "static" IP by his ISP, that address also changes periodically and ISPs may not retain the IP data for long.

The ephemeral nature of IP data is a very real problem to those who bring Doe suits alleging injury from online activity. A delay of 30 days before an ISP is contacted to preserve or produce IP data can mean that the ability to track down the online actor disappears forever.

Courts have generally responded quickly to the RIAA's subpoena requests. The court in *Elektra Entertainment Group Inc. v. Does 1-7*, Civil Action No. 04-607 (GEB) (D.N.J.), issued the order for discovery on Feb. 18, 2004, the day after the action was filed. In *Capitol Records, Inc. v. Does 1-250*, Civil Action No. 04-472 (LAK) (S.D.N.Y., Jan. 24, 2004), the discovery order was issued five days after the case was filed.

In these RIAA suits, the form of order for subpoena provided by the RIAA to courts does not

require the ISP to first notify the customer of the subpoena request and give the customer the chance to move to quash the subpoena before the ISP reveals the customer's identity.

Many ISPs notify customers of subpoena requests as part of their ordinary course of business before producing account information in response to subpoenas. Some Internet portals such as AOL and Yahoo! delay producing account information for 15 days following e-mail notice to the customer of the subpoena request.

### First Amendment Arguments

In some of the recent RIAA Doe cases, the Electronic Freedom Foundation (EFF), a First Amendment advocacy group, has intervened on behalf of the defendants.

EFF argues there should be no disclosure of account information until the ISP first notifies the customer of the subpoena request so the customer can decide whether to obtain counsel to oppose disclosure of the customer's identity.

In one pending lawsuit brought by the RIAA, *Sony Music Entertainment Inc. v. Does 1-40*, Civil Action No. 04-473 (DC) (S.D.N.Y.), EFF's motion papers argued that the First Amendment protects the right to engage in online activity anonymously and that the subpoenas, which seek to "unmask" online users, threaten, or at least implicate, First Amendment rights.

In support of this argument, the EFF relies on judicial decisions in the context of cyber defamation — sometimes called "cybersmear" — where some jurisprudence exists regarding applications for "identity discovery."

In *Dendrite International, Inc. v. Doe*, 775 A.2d 756 (N.J. App. Div. 2001), cited by EFF in its Sony motion papers, the corporate plaintiff accused the Doe defendant of defamation based on a message posted anonymously on Yahoo! Finance to the effect that the chairman of the company was "shopping" the company and had inflated its earnings.

The court held that, before disclosing to the plaintiff any identifying information about the anonymous poster, an effort should be made to give notice to the poster of the lawsuit and the application for identity discovery.

The court also held that, because First Amendment rights were implicated by the request to "unmask" the anonymous defendant, no order for discovery should be issued unless

the court is satisfied that the plaintiff's claims against the anonymous defendant were viable. (See also *La Societe Metro Cash & Carry France v. Time Warner Cable*, 36 Conn. L. Rptr. 170 (Conn. Super. 2003); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D.Cal. 1999).

The Court in *Dendrite* held that the defamation claim was not viable and denied the request for identity discovery.

### Industry Response

The RIAA argues that cyber defamation cases are inapplicable to its recent Doe suits because there is no First Amendment right to engage in copyright infringement.

The group also argues that its members are suffering irreparable harm each time a file-sharer engages in the illegal copying of a copyrighted work. Further, RIAA asserts that ISP customers have waived any anonymity by disclosing their identity to the ISP itself, just as telephone company customers have no expectation that phone companies will not disclose records of their phone calls.

Additionally, RIAA points out that file-sharers on P2P networks are in a particularly poor position to talk about a right to anonymity because of the nature of file-sharing itself. Given that a file-sharing customer "opens his computer to permit others, through peer-to-peer file sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world." *In re Verizon Internet Servs., Inc.*, 257 F. Supp.2d 244, 267 (D.D.C. 2003), rev'd on other grounds, 351 F.3d 1229 (D.C. Cir. 2003).

In the *Sony* case, Southern District Judge Denny Chin entered a form of order granting the discovery but requiring the ISP to give notice to the subscriber that a subpoena had been served, leaving subscribers a short period within which to move to quash the subpoena before the account information was to be turned over to the RIAA.

Judge Chin's approach is a sensible compromise provided that the applicant for the subpoena receives some assurance from the ISP that IP data will be preserved during any period of delay.<sup>2</sup> This can be accomplished by including a "preservation of evidence" provision in the court order allowing the subpoena. Indeed, it is wise for copyright holders and other victims of online injury to serve a written "preservation of evidence" demand upon an ISP as soon as the IP data can be ascertained.

It would also appear to be in the best interest of ISPs to defer producing customer data to record industry plaintiffs until after the ISP first lets the customer know of the request for subpoena and gives the customer time to retain counsel.

Customers may claim an expectation that ISPs will protect personal information about online activity. By giving notice to the customer of the subpoena, the ISP also may reduce the possibility that it later will face a lawsuit by a user alleging that the ISP erroneously, or otherwise without good cause, revealed the user's identity and information about the user's online behavior.

Thus, courts faced with requests for Doe subpoenas should order the ISP (i) to preserve all information relating to the IP addresses in question and (ii) to give notice to the customer of the lawsuit and subpoena.

That same order should authorize issuance of the subpoena by the ISP compelling production of account information after a short period has elapsed. During that interval, the Doe defendant can decide whether to engage counsel to move to quash the subpoena or perhaps consider entering into an immediate settlement with the copyright holder.

Many Doe defendants are pursuing the latter alternative. In the *Sony* case, the RIAA named 40 Doe defendants. After obtaining ISP account information for some of them, the RIAA filed separate dismissals against individual defendants, indicating that the dismissed defendants had reached a settlement with the RIAA.



1. The recent cases have been filed by individual records companies but appear to be directed by RIAA. For ease of reference, this article refers to the plaintiffs as RIAA.

2. While a short delay is not unduly prejudicial where IP data is known and an ISP honors a demand for preservation of associated account information, it can cause prejudice in the following *Dendrite*-style fact pattern: The plaintiff is defamed in an anonymous message on Yahoo!; Yahoo! delays producing IP data associated with a defamatory message; during the period of delay, the author's ISP, having no knowledge of the subpoena request, discards the account information associated with the IP address which the customer used to post the message. Once the ISP deletes the historic IP data, it may become impossible to tie the customer to the message.