REPRINTED FROM:
NYSBA
SPRING 2004 | VOL. 10 | NO. 1

Commercial and Federal Litigation Section Newsletter
A publication of the Commercial and Federal Litigation Section of the New York State Bar Association

Strategies for Unmasking the 'Anonymous' Internet User

By Rajen Akalu and Peter J. Pizzi

The internet poses unique challenges for litigators. Among these challenges is the identification of defendants in order to initiate legal proceedings. These issues have been brought most sharply into focus by the vigorous pursuit of alleged copyright infringement by the Recording Industry Association of America (RIAA).

This article discusses the various procedural mechanisms used by RIAA in order to compel internet service providers (ISPs) to disclose the identity of its subscribers using peer-to-peer (P2P) file-sharing software such as KaZaA.

Background

In the digital context copyright material can be reproduced and disseminated instantaneously at marginal costs and with perfect fidelity to the original. File sharing programs such as Napster permitted users to download and share files on their computers using (P2P) technology. Napster operated a centralized database which served an indexing function.[1] The fact that the system was centralized allowed an injunction to be successfully obtained against Napster to enjoin it from facilitating the sharing of music files.

But as Napster closed (and resurfaced as a paid service)[2] KaZaA and other P2P file sharing software programs emerged. Unlike Napster, KaZaA has a decentralized structure. The searching of files relies on the indexing by end-users themselves.

The decentralized nature of P2P networks has made it more difficult to challenge their activities in courts of law because they are not "controlled" by any one entity. There are two factors that can overcome this obstacle however:

> (a) The lack of end point anonymity – a computer's identity or Internet Protocol (IP) address readily available; Internet Service Providers can link the users IP address with its customer records and subsequently reveal the identity of the user; and
>
> (b) Free riding – the fact that users commonly set their computers to download but not share files with other users. This results in a smaller number of computers holding large collections of illicit copyright material which are in turn made available to other users. Targeting these users will invariably frustrate the network.[3]

These factors have lead to lawsuits being filed against individuals using P2P to "share" copyright protected works. These actions are being brought under the Digital Millennium Copyright Act (DMCA).[4]

The *RIAA v. Verizon* Case

In *Recording Industry Association of America v. Verizon Internet Services*,[5] decided late last year, the D. C. Circuit found that subpoena provision section 512(h) of the DMCA did not authorize the issuance of a subpoena to an ISP which was alleged to have provided the means of communication but which could not be said to have control over material located on its customers' computer hard drives.

Section 512(h) permits the copyright owner (or its agent such as the RIAA) to request the clerk of any United States district court to issue a subpoena to an ISP for the identification of an alleged infringer. The issuance of the subpoena is contingent on filing of (i) a notification of the claimed infringement of copyrighted work(s), (ii) the proposed subpoena directed to the ISP, and (iii) a sworn declaration that the purpose of the subpoena is "to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting" rights pursuant to copyright law.

The Court pointed out that, irrespective of the RIAA's motion to compel pursuant to section 512(h), "the ISP can neither 'remove' nor 'disable access to' the infringing material because that material is not stored on the ISP's servers" but rather on customer hard drives.[6]

It further found that Congress could not have foreseen the application of section 512 (h) to P2P file-sharing when the DMCA was enacted. Had it anticipated this development, the subpoena provision might have been drafted more broadly.[7]

The court sympathized with the record industry's plight but felt constrained by the language and intent of the DCMA, as Judge Ginsburg observed:

> 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 DMCA in order 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 software industries.[8]

Unmasking the Doe – the Record Companies' New Tactic

In response to the D.C. Circuit's decision in *Verizon*, record companies have begun to commence "Doe" suits in federal courts around the country, accusing unnamed defendants of copyright infringement on P2P networks. In January and February, 2004, over a dozen such lawsuits were filed in the name of individual record companies against "Doe" defendants.[9] The complaints were accompanied by motion papers seeking a court order authorizing the service of a subpoena pursuant to Rule 45, Fed. R. Civ. P., directed to ISPs. The supporting motion papers indicated that RIAA traced file-sharing activity to "IP" addresses assigned to users who were customers of particular ISPs. The ISPs could be identified because each ISP is assigned a particular range of IP addresses.

In *Elektra Entertainment Group Inc. v. Does 1–7*, filed in the District of New Jersey,[10] the form of order tendered to the Court sought the following discovery:

> ORDERED that Plaintiffs may serve immediate discovery on RCN to obtain the identity of each Doe Defendant by serving a Rule 45 subpoena that seeks information sufficient to identify each Doe Defendant, including the name, address, telephone number, e-mail address, and Media Access Control addresses for each defendant.[11]

In *Capitol Records, Inc. v. Does 1–250*, filed in the Southern District of New York, the plaintiff sought similar relief[12] and in motion papers stressed need for the issuance of an immediate subpoena to the ISP citing the practice of ISPs commonly erasing the identifying IP information every week or ten days.[13] In *Elektra*, the Court issued the order for discovery on February 18, 2004, the day after the action was filed. In *Capitol Records*, the discovery order was issued five days after the case was filed.

Cybersmear to the Rescue?

How should courts respond when presented with an application for a subpoena in such Doe lawsuits? The Federal Rules of Civil Procedure are largely silent on the criteria courts are to apply in ruling on an application for discovery before the summons and complaint has been served.

Perhaps courts should look to cases in the context of cyber defamation or "cybersmear," where a body of jurisprudence has accumulated about how courts are to decide applications for "identity discovery"–discovery needed in order for the plaintiff to "identify" the defendant. First Amendment advocates such as Public Citizen and the Electronic Freedom Foundation[14] have intervened in the most notable of such cases and successfully argued as *amici* that, before disclosing any information to the record company plaintiff, an effort should be made to give notice of the lawsuit to the anonymous defendant. Further, such organizations argue that, before an order for "identity discovery" is entered, the Court must be satisfied that the claims of the plaintiff against anonymous defendant are viable when considered under the kind of scrutiny applicable to a motion for summary judgment.[15]

In *Dendrite v. Doe*, the corporate plaintiff accused the defendant of defamation based upon a message posted anonymously on Yahoo! Finance to the effect that the Chairman of the company was "shopping" the company and had inflated earnings.[16] As one of the pre-requisites to identity discovery, the Court required the plaintiff to post notice of the lawsuit in the Yahoo! Finance chatroom where the message originally appeared.[17] After this prerequisite had been satisfied, the Court then considered whether the allegations in the complaint against the anonymous defendant were viable according to *prime facie* standard.[18] The Court held that the corporate plaintiff had failed to prove *harm* to its business from the posting on Yahoo! Finance about the company. Since proof of harm is a requirement for a viable defamation claim in New Jersey, the Court denied the application for discovery.[19]

In the "cybersmear" cases such as *Dendrite*, courts have recognized that anonymous online activity implicates important First Amendment rights of free speech, association, and privacy.[20] These courts have also wrestled with the notion that identity discovery is sometimes the goal of the lawsuit itself. In the P2P context, once the file sharer is "unmasked," the case essentially is over given that few file-sharers will have the resources to challenge the RIAA and major record labels pitted against them. If the real battle in these cases is over the identity of the anonymous defendant, a more rigorous scrutiny is in order before the Doe defendant is unmasked.

Record companies now suing P2P file-sharers arguably will have an easier time satisfying the *prima facie* standard than did the corporate plaintiff in *Dendrite*. Still, given the First Amendment interests involved, courts should consider a three-step procedure. First, the court should order the ISP where the file-sharer operates to preserve all information relating to the IP addresses cited in the motion papers.[21] Perhaps this same order should direct the file-sharer also to preserve all data on his or her computer. Second, the court should order the ISP to give notice of the lawsuit, and the application for identity discovery, to the customer in question. Third, after a reasonable period has passed (perhaps fifteen days), the court may entertain the application for identity discovery and, if satisfied that the complaint alleges a viable claim for copyright infringement, enter an order compelling the ISP to disclose the customer's identity.

Further, an ISP facing a court order seeking discovery of customer identity should delay responding to the subpoena until after it gives notice to the customer making it aware that the subpoena had been served, regardless of whether the court has ordered such notice. This has been the routine practice of AOL, Yahoo! and other web portals when served with subpoenas in cybersmear cases. By giving such notice, the ISP can reduce the possibility that it will face some kind of later invasion of privacy 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.

It is worth noting in this context that the protection of personal information is a central pillar of trust in the on-going business relationship between the ISP and its customer. In addition to being a good business practice, giving notice to the customer will protect the ISP from facing possible privacy claims from customers. Subscribers may cite the Cable Communications Privacy Act[22] which can be read as permitting a cable operator to disclose subscriber information only after the operator first gives notice to the subscriber that it has been served with a court order requiring disclosure of the subscriber's identity. Imposing a requirement that the subscriber receive notice of the request for identity discovery before his or her identity is disclosed will reduce the ISP's exposure to such a claim.

Endnotes

1. *A&M Records, Inc. v Napster, Inc.*, 284 F.3d 1004 (9th Cir. 2002).
2. *See* http://www.napster.com/ (last visited March 10, 2004).
3. Biddle, P., England, P., Peinado, M., and Willman, B. *The Darknet and the Future of Content Distribution,* in Proceedings of the 2002 ACM Workshop on Digital Rights Management (Washington, DC, Nov. 18, 2002).
4. Pub. L. No. 105-304, 112 Stat. 2860 (amending title 17 of the U.S.C.).
5. 351 F.3d. 1229 (D.C. Cir., Dec. 19, 2003).
6. *Id.* at 1235 *per* Ginsburg C.J.
7. *Id.* at 1238.
8. *Id.*
9. A list of such lawsuits appears at the Electronic Freedom Foundation's website at http://www.eff.org/IP/P2P/riaa-v-thepeople.php.
10. *Elektra Entertainment Group Inc. v. Does 1–7*, U.S.D.C., D.N.J., Civil Action No. 04–607 (GEB); *Capitol Records, Inc. v. Does 1–250*, U.S.D.C., S.D.N.Y., Civil Action No. 04–472 (LAK).
11. In a local area network (LAN) or other network, the MAC (Media Access Control) address is a computer's unique hardware number. On a local area network, the MAC is the same as the machine's Ethernet address.) When connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the local area network. *See* http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212506,00.html.
12. Order entered January 26, 2004 in *Capitol Records, Inc. v. Does 1–250*, U.S.D.C., S.D.N.Y., Civil Action No. 04–472 (LAK).
13. Where an ISP uses a system of "dynamic" (as opposed to "static") IP addresses, IP information is purged within a matter of weeks or less as IP addresses are recycled from one user to another. A data preservation demand served upon the ISP should serve to preserve request that the ISP preserve, permitting courts to act upon the subpoena application in a more leisurely fashion.
14. Information regarding these organizations is available at http://www.citizen.org and http://www.eff.org/ respectively (last visited March 12, 2004).
15. See *La Societe Metro Cash & Carry France v. Time Warner Cable*, 2003 WL 22962857 (Conn. Super. Ct.); *Melvin v. Doe*, 49 Pa.D.&C.4th 449 (2000), *appeal quashed*, 789 A.2d 696, 2001 Pa.Super. 330 (2001), *appeal reinstated*, 836 A.2d 42 (Pa. 2003); *Dendrite v. Doe*, 775 A.2d 756 (N.J. App. Div. 2001); *Columbia Ins. Co. v. Seescandy.com*, 185 FRD 573 (N.D.Cal. 1999).
16. *Dendrite v. Doe*, 775 A.2d 756, 763 (N.J.App. 2001).
17. *Id*. at 760.
18. *Id*.
19. *Id*. at 764.
20. *See Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
21. This leads to the question whether the expense of preserving such data (i) is measurable and (ii) should be borne by the ISP.
22. 47 U.S.C. 551.

Rajen Akalu currently works for the Centre for Innovation Law and Policy at the University of Toronto and is the Bell Universities Lab Manager (Law). He is a member of the Internet and Litigation Committee.

Peter J. Pizzi is a partner in Connell Foley LLP in New York City and Chair of the Section's Internet and Litigation Committee.

REPRINTED WITH PERMISSION FROM THE: *COMMERCIAL AND FEDERAL LITIGATION SECTION* NEWSLETTER, SPRING 2004, VOL. 10, NO. 1, PUBLISHED BY THE NEW YORK STATE BAR ASSOCIATION, ONE ELK STREET, ALBANY, NEW YORK 12207.