January 16, 2012

Copyright Doe Defendant Can't Quash Disclosure Subpoena Anonymously—Hard Drive Productions v. Does (Guest Blog Post)

By Guest Blogger Elliott Alderman with brief comments from Eric

[Eric's introductory note: Elliott Alderman is an IP attorney in Washington DC. I asked if he could guest-blog this opinion after calling it to my attention.]

Hard Drive Productions, Inc. v. Does 1-1,495, Civil Action No. 11-1741 (D.C. D.C. Dec. 21, 2011)

Overview: A DC Magistrate Judge recently ruled that a defendant cannot file anonymous motions to quash disclosure subpoenas in copyright file-sharing case. This ruling invites discovery abuses--and kicks due process.

The fragile balance between copyright owners enforcing their rights and the privacy interests of IP address owners was upended recently in *Hard Drive Productions, Inc. v. Does 1-1,495*, Civil Action No. 11-1741 (2011). There, the magistrate held that individuals who subscribe to the Internet through ISPs have no expectation of privacy in their subscriber information, since they have already disclosed this information to their service providers. So when copyright owners file disclosure subpoenas seeking subscriber information, local district court rules require that responding IP address owners must publicly identify themselves as part of filing a motion to quash.

There are two separate levels of privacy involved here: (1) public knowledge (including opposing counsel) of the IP address owner's identity, and (2) the court's knowledge of the parties involved in an action before it. A simple solution to the considerable detriment posed to subpoenaed parties is to allow motions to be filed under seal. At this stage, it is only discovery, not adjudication on the merits of the underlying claims, and there is no public benefit to disclosure before consideration of the motions.

Some background: As content owners move from suing download sites for inducement liability to a model of filing reverse class actions against unnamed individual users of P2P networks, discovery of infringers becomes crucial. However, content monitoring software, at best, may associate a digitally marked file with an IP address, but does not identify the owner of the account. And, significantly, the owner of the account is not, by definition, an infringer. So with IP addresses in hand, copyright owners must file disclosure subpoenas with ISPs to get the subscriber information associated with the identified IP addresses.

Typically, consistent with due process (and common sense), IP address owners responding to a disclosure subpoena have the right to preserve their anonymity while a judge reviews the propriety of the class action and the corresponding subpoena. Without the protection of anonymity, a motion to quash a disclosure subpoena is rendered moot, since disclosure of personal information on a public docket reveals the name and address information sought by the subpoena. *See Achte/Neunte Boll Kino Beteiligungs GMBH & Co. v. Does 1-4,577*, 736 F. Supp. 2d 212, 215 (D.D.C. 2010). Ironically, *Achte/Neunte* is one of the cases cited by the magistrate in support of public disclosure.

For a number of reasons, *Hard Drive* makes no sense. A subpoenaed owner essentially no longer has a right to contest disclosure, since challenging the merits of the discovery process reveals the very thing sought in discovery – his identity. And even if the judge later holds that the owner was misjoined, that an IP address is not an infringer, or any of the other bases that courts throughout the country are using to dismiss file-sharing defendants and kill these suits, plaintiffs have the personal information that they need to harass presumptively innocent parties. Worse still, plaintiffs will be encouraged to withdraw subpoenas before judges evaluate their merits, since the subpoenaed information will already be in hand.

As noted above, the *Hard Drive* magistrate also based his holding on Local Rule 5.1, which requires that all parties who file pleadings and papers with the district court must provide their name and full residence address, even if they are seeking to

proceed anonymously. Judge Bates, who had assigned the case to the magistrate, originally ordered that motions to quash would remain under seal *even if* the moving party lost. How about a Solomonic compromise? Allow motions to be filed under seal, then only if the motion is denied would subscriber information be released, since the ISP is going to disclose the information anyway. Certainly there are policy reasons supporting the requirement that parties identify themselves to the court -- not the least of which is that it has no way of communicating with unrepresented Does – but permitting sealed motions balances the interests of copyright owners seeking to vindicate their rights against the privacy rights of IP address owners.

Moreover, the central premise of the decision, that there is no expectation of privacy in business transactions where information is disclosed to a third party, defies logic. One also shares information with telephone and insurance companies, and medical doctors – third parties all – but an expectation of privacy remains. Moreover, courts have implicitly recognized a privacy interest in ISP subscriber information, holding that copyright owners may not use the DMCA's takedown notice-subpoena provisions to discover subscriber identities. *See Recording Industry Association of America v. Verizon Internet Services, Inc.*, 351 F.3d 1299 (D.C. Cir 2003); *In re Charter Communications, Inc.*, 393 F.3d 771 (8th Cir. 2005). And although it may be argued that when copyright infringement is at issue there is no free speech right to anonymity, see e.g. *Sony Music Entertainment, Inc. v. Does*, 326 F. Supp. 2d 556 (S.D.N.Y. 2004), the extortionate nature of the file-sharing cases is such that fairness would dictate that IP address owners should be able to anonymously defend against inclusion in classes of unrelated others.

Further, even assuming that an individual has no reasonable expectation of privacy in his subscriber information, he certainly does in his choice of movies. Part of the copyright troll business model, particularly for pornographic films, is the threat of publicly associating an individual with his private tastes. I have represented a number of owners who have had their routers hacked or had tenants or other unauthorized

parties who used their Wi-Fi connections. With or without legal liability, too many of these parties have settled because privacy is a more expensive currency than cash.

In fact, in other contexts where there is the potential for stigma or embarrassment, courts typically evaluate the merits of the underlying case before requiring disclosure of confidential information, like a person's identity. *See, e.g. Doe v. Smith*, 429 F3d 706 (7th Cir. 2005). The potential for harm to defendants in file-sharing cases is worse, however, because in addition to whatever shame or stigma attaches to being labeled an infringer or, worse, a porn hound (I think that's the legal term), there are immediate legal consequences to stripping anonymity. Not permitting sealed motions is like having discovery first, then later evaluating its legitimacy.

Finally, the importance of the anonymous motion is intertwined with the architectural problems with the reverse class action model generally. This is not a white hat/black hat debate between content creators and piracy. Rather, the file-sharing cases are about the economics of joining unrelated parties in a class as a cost-effective way to pursue often non-meritorious actions, where secondary parties who are not infringers become the collateral damage. A number of court have dismissed these actions on a variety of grounds, including that:

* IP address owners are not intrinsically infringers. *See VPR Internationale v. Does 1-1017*, 2:2011cv02068 (C.D. Ill. 2011) (an IP address is not a person)
* different owners have different defenses; and
* unrelated owners do not act in concert by using a P2P program. *K-Beech, Inc. v. John Does 1-85*, Civil Action No. 3:11cv469 (E.D. Va. 2011); *Raw Films, Ltd. V. John Does 1-32*, Civil Action No. 3:11cv532 (E.D. Va. 2011); *Hard Drive Productions, Inc. v. Does*, No. C-11-01566 (N.D. Cal. 2011).

Moreover, the reliability of monitoring programs is suspect, *Challenges and directions for monitoring P2P File Sharing Networks*, University of Washington Technical Report, UW-CSE-08-06-01, and because a number of ISPs use dynamic IP addresses (where an IP address is rotated between several users) and "infringements" are generally date-

and time-stamped, the odds of mistakenly associating a particular IP address with the "infringement" is greatly increased.

All this for want of a sealing motion!

Eric's Comments

This is a bad ruling. The court has guaranteed that the copyright plaintiff can unmask defendants simply by asking for a subpoena—either the subpoena is granted or the defendant reveals him/herself to fight the subpoena. That's not the way the system is supposed to work. By creating a no-recourse situation for anonymous/pseudonymous defendants, the court has stripped them of essential due process rights. And, as we know, plaintiffs able to unmask defendants often can take advantage of substantial extra-judicial remedies, such as the public embarrassment factor in porn copyright cases. Thus, this ruling unfairly screws over anonymous defendants in these cases. It needs to be fixed.

For more on the topic, see Lior Strahilevitz's paper Pseudonymous Litigation.