E-FILED
Tuesday, 18 September, 2012 04:27:57 PM
Clerk, U.S. District Court, ILCD

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS

MALIBU MEDIA, LLC,	)	
	)	
Plaintiff,	)	Civil Case No. 1:12-cv-01188-JES-JAG
	)	
v.	)	
	)	
JOHN DOES 1-34,	)	
	)	
Defendants.	)	
	)	

PLAINTIFF'S MEMORANDUM IN OPPOSITION TO OBJECTION TO SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS, OR TO PERMIT INSPECTION OF PREMISE IN A CIVIL ACTION [DKT. #8]

I. INTRODUCTION

Plaintiff respectfully requests the Court deny Defendant's Motion because he has not provided a valid reason for this Court to quash the subpoena issued to his ISP. At this stage of the litigation process, Plaintiff has no other option but to file suit against the owners of these IP addresses to obtain the infringers identities. If this Court were to follow Defendant's rationale, Plaintiff would have no recourse against the mass copyright infringement it suffers on a daily basis. Your Honor Previously stated, "[b]ecause of the very nature of internet infringement, it is often the case that a plaintiff cannot identify an infringer in any way other than by IP number. Given the substantial federal policy underlying copyright law, it would be a travesty to let technology overtake the legal protection of that policy." Order DE #6. "While we would like to think that everyone obeys the law simply because it is the law and out of a sense of obligation, we also know that laws without penalties may be widely ignored."[1] Plaintiff has suffered great

[1] Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks Statement of Marybeth Peters The Register of Copyrights before the Committee on the Judiciary 108th Cong. (2003) available at http://www.copyright.gov/docs/regstat090903.html

harm due to infringements committed by thousands of residents in this District and has no option but to file these suits to prevent the further widespread theft of its copyright.

II. THIS COURT SHOULD NOT QUASH THE SUBPOENA

This Court has previously determined that Plaintiff has established good cause to issue a Rule 45 subpoena on Defendant's ISP prior to a Rule 26(f) conference so that Plaintiff may obtain Defendant's identity. There are limited circumstances under which the federal rules allow a Court to quash a subpoena. Rule 45(c)(3) provides that a court must modify or quash a subpoena that fails to allow a reasonable time to comply; requires a non-party to travel more than 100 miles (except for trial within the state); requires disclosure of privileged materials; or, subjects a person to undue burden. See Fed. R. Civ. P. 45(c)(3)(A)(i-iv). The Rule also provides for circumstances in which a court may modify or quash a subpoena. These circumstances are when the subpoena requires disclosure of trade secrets; disclosure of certain expert opinions; or, requires a nonparty to incur substantial expense to travel more than 100 miles to attend a trial. See Fed. R. Civ. P. 45(c)(3)(B)(i-iii). Defendant has failed to demonstrate any of these criteria and accordingly his motion to quash should be denied.

"The party seeking to quash the subpoena bears the burden of demonstrating that the requirements of Rule 45 are satisfied. Courts have described this as a heavy burden." Malibu Media, LLC v. John Does 1-15, CIV.A. 12-2077, 2012 WL 3089383 (E.D. Pa. July 30, 2012) (internal citations omitted). The Northern District of Illinois has recognized that "[w]hen a subpoena is directed to a nonparty, any motion to quash or modify the subpoena generally must be brought by the nonparty against which it is directed. A party to the action does not have standing to challenge a subpoena directed to a nonparty unless that party claims a personal right or privilege regarding the production commanded by the subpoena." Barker v. Local 150, Int'l

Union of Operating Engineers, AFL-CIO, 08 C 50015, 2010 WL 934068 (N.D. Ill. Mar. 11, 2010) (internal citations and quotations omitted).

Plaintiff's interest in receiving the subpoenaed information outweighs any privilege Defendant may have. It is now well known law that "First Amendment privacy interests are exceedingly small where the 'speech' is the alleged infringement of copyrights." Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 8 (D.D.C. 2008) see also Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. Does 1-4,577, No. 10-453, 2010 U.S. Dist. LEXIS 94594, at *10 n.2 (D.D.C. Sept. 10, 2010) ("the protection afforded to such speech is limited and gives way in the face of a prima facie showing of copyright infringement"); West Bay One, Inc. v. Does 1-1653, 270 F.R.D. 13, 16 n.4 (D.D.C. July 2, 2010) (using the same language as Achte/Neunte, 2010 U.S. Dist. LEXIS 94594, at *10 n.2); Sony Music Entertainment v. Does 1-40, 326 F. Supp. 2d at 567 (First Amendment right of alleged file-sharers to remain anonymous "must give way to the plaintiffs' right to use the judicial process to pursue what appear to be meritorious copyright infringement claims."); Elektra Entm't Group, Inc. v. Does 1-9, No. 04-2289, 2004 WL 2095581, at *4-5 (S.D.N.Y. Sept. 8, 2004) (finding that First Amendment right to anonymity overridden by plaintiff's right to protect copyright).

The Northern District of Illinois has expressly adopted the test laid out in Sony Music in determining in a nearly identical case that "each of the five factors weighs against the Putative Defendants and in favor of disclosing their identifying information in compliance with the subpoenas." First Time Videos, LLC v. Does 1-500, 276 F.R.D. 241, 249 (N.D. Ill. 2011). The factors to be considered are under Sony Music are

> (1) a prima facie claim of infringement; (2) the specificity of the information sought from the ISP; (3) a lack of alternative means of obtaining that information; (4) a "central need" for the information in order to bring the claim; and (5) the expectation of privacy held by the objecting party.

Id. (citing Sony Music).

After weighing the above factors the court ultimately found, on essentially identical facts to the case at hand, that the Defendant's interest in keeping his identifying information private was far outweighed by the plaintiff's need for the information and therefore denied the motion to quash.

> The Court concludes that the identifying information subpoenaed neither qualifies for protection as "privileged" nor is otherwise protected under the First Amendment right to engage in anonymous speech on the Internet. Consequently, the Doe discovery subpoenas will not be quashed on the basis that compliance will require disclosure of privileged or other protected matter.

First Time Videos, LLC v. Does 1-500, 276 F.R.D. 241, 247 (N.D. Ill. 2011).

Accordingly, the Sony Music test weighs in favor of Plaintiff here as well. Courts have recognized that the expectation of privacy of individuals who have freely conveyed their identifying information to ISPs in signing up for internet service is low, if not inexistent. "[C]ourts analyzing the expectation of privacy possessed by internet users engaging in online file-sharing have concluded that such expectation is at most minimal because those individuals have already voluntarily given up certain information by engaging in that behavior." Raw Films, Ltd. v. John Does 1-15, CIV.A. 11-7248, 2012 WL 1019067 (E.D. Pa. Mar. 26, 2012). Even if this Defendant has retained a reasonable expectation of privacy in his subscriber information, Plaintiff has no other way to pursue its valid claims for copyright infringement. Obtaining the identifying information of Doe Defendants is essential to Plaintiff's ability to protect its copyright. Therefore, Plaintiff respectfully requests this Court deny Defendant's motion.

Additionally, Plaintiff has requested only the identifying information of the Defendants from their ISPs.

> The Court found good cause for ordering that discovery, *see* Fed.R.Civ.P. 26(b)(1), because the plaintiff showed that a subpoena seeking the subscriber information associated with the allegedly infringing IP addresses would be the

> only way for the plaintiff to identify the proper defendants in this case and proceed with its claims against them.[3] *See* Declaration of Tobias Fieser ¶ 9, 23, Pl.'s Mot. Ex. The information sought is thus highly relevant to the plaintiff's claims.

Raw Films, Ltd. v. John Does 1-15, CIV.A. 11-7248, 2012 WL 1019067, at *6 (E.D. Pa. Mar. 26, 2012). That court also noted that Fed. R. Civ. P. 26(b)(1) permits parties to obtain discovery of "the identity and location of persons who know of any discoverable matter." Id. at *14. When addressing the issue of whether the infringer is the account holder of the IP address, the Court stated "[t]hese are not grounds on which to quash a subpoena otherwise demonstrated to be proper. The moving Doe may raise these and any other nonfrivolous defenses in the course of litigating the case." Id.

Defendant relies on the Eastern District of New York opinion where Judge Brown questioned the likelihood the infringer was the owner of the IP Address. See DE #8 at ¶ 3. Plaintiff respectfully disagrees with Magistrate Judge Brown's opinion and believes that recent technological advances make it more likely that a wireless account will be secured and can easily be traced to a household where the subscriber either is the infringer or knows the infringer. Recently, PC Magazine published an article regarding the scarcity of open wireless signals. "These days, you are lucky to find one in 100 Wi-Fi connections that are not protected by passwords of some sort."[2] The author continues to explain why routers are now more likely to be secured. "The reason for the change is simple: the router manufacturers decided to make users employ security with the set-up software. As people upgrade to newer, faster routers, the wide-open WiFi golden era came to an end."[3] This article, published on March 26, 2012, runs contrary to Judge Brown's assertions and supports the idea that most households have closed, protected wireless that is not likely to be used by a neighbor or interloper.

[2] See Free Wi-Fi is Gone Forever www.pcmag.com/article2/0,2817,2402137,00.asp
[3] Id.

Further, Plaintiff uses the same process as Federal Law Enforcement to identify cyber crimes. In a Statement of Deputy Assistant Attorney General Jason Weinstein before the Senate Judiciary on Privacy, Technology and the Law, he discusses how Federal law enforcement use IP addresses to identify an individual.

> When a criminal uses a computer to commit crimes, law enforcement may be able, through lawful legal process, to identify the computer or subscriber account based on its IP address. This information is essential to identifying offenders, locating fugitives, thwarting cyber intrusions, protecting children from sexual exploitation and neutralizing terrorist threats.[4]

While, as Defendant suggests, this process may not be 100% accurate, it is the most accurate and likely way to identify the person responsible for the use of that IP address. Indeed, it is the only way.

The Eastern District of Pennsylvania directly addressed whether an IP address was sufficient to identify the infringer.

> The Court acknowledges that Verizon's compliance with the subpoena may not directly reveal the identity of an infringer. Indeed, the subscriber information Verizon discloses will only reveal the account holder's information, and it may be that a third party used that subscriber's IP address to commit the infringement alleged in this case.

Raw Films, Ltd. v. John Does 1-15, CIV.A. 11-7248, 2012 WL 1019067 (E.D. Pa. Mar. 26, 2012). (Internal citations omitted). The Court went on to note that while the IP address did not guarantee the subscriber was the infringer, "[t]he subpoena is specific enough to give rise to a reasonable likelihood that information facilitating service upon proper defendants will be disclosed if the ISPs comply." Id. The Northern District of Indiana additionally noted "objections such as these are essentially irrelevant and premature because they go to the merits of Plaintiff's claims and do not address the propriety vel non of the subpoenas." Third Degree

[4] Statement of Deputy Assistant Attorney General Jason Weinstein Before the Senate Judiciary Subcommittee on Privacy, Technology and the Law available at www.justice.gov.

Films, Inc. v. Does 1-2010, 4:11 MC 2, 2011 WL 4759283 (N.D. Ind. Oct. 6, 2011) (internal citations omitted).

The only way to enforce one's copyrights against online infringement is to subpoena the identity of the subscriber whose internet was used to commit the infringement. "[Plaintiff] has a critical need for this information so it may proceed with its suit, remedy its losses, and prevent further infringement." Id. Without this ability, copyright owners would have a right without a remedy. Any such state of affairs would violate Chief Justice Marshall's often cited rule that "the very essence of civil liberty certainly consists in the right of every individual to claim the protection of the laws, whenever he received an injury." Marbury v. Madison, 1 Cranch 137, 1803 WL 893, *17 (U.S. 1803).

III. CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court deny the subject motion.

Dated: September 18, 2012

Respectfully submitted,
NICOLETTI & ASSOCIATES, PLLC

By: /s/ *Paul J. Nicoletti*

Paul J. Nicoletti, Esq. (P44419)
36880 Woodward Ave, Suite 100
Bloomfield Hills, MI 48304
Tel: (248) 203-7800
Fax: (248) 203-7801
E-Fax: (248) 928-7051
Email: paul@nicoletti-associates.com
Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on September 14, 2012, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF and that service was perfected on all counsel of record and interested parties through this system.

By: /s/ *Paul J. Nicoletti*