

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC,	:	
	:	
Plaintiff	:	Civil Action No. 5:12-cv-02088
	:	
vs.	:	
	:	
JOHN DOES 1-22,	:	
	:	
Defendants	:	

**DEFENDANT, JOHN DOE NO. 14’S, MEMORANDUM OF LAW IN SUPPORT OF
MOTION TO VACATE ORDER GRANTING LEAVE TO FILE SUBPOENA, TO
QUASH SUBPOENA, AND, ALTERNATIVELY, FOR PROTECTIVE ORDER**

Defendant, John Doe No. 14, by and through undersigned counsel, respectfully submits this Memorandum of Law in Support of Defendant’s Motion to Vacate Order Granting Leave to File Subpoena, to Quash Subpoena, and, Alternatively, for Protective Order.

I. INTRODUCTION

The instant case demonstrates a trend that is becoming commonplace among online, adult entertainment businesses and lawsuits regarding their copyrighted material. It involves speculative allegations of copyright infringement and questionable use of the legal system to quickly gain profit via the generation of settlements from defendants threatened by the potential of large awards, public embarrassment, and notoriety which attaches to defendants when identified and associated with illegally downloading pornographic films. This case, along with hundreds of similar cases nationwide, demonstrates how the plaintiffs use the courts to coerce quick and profitable settlements out of intimidated and embarrassed defendants. These actions are part of a “nationwide blizzard of civil actions brought by purveyors of pornographic films alleging copyright infringement by individuals utilizing a computer protocol known as a BitTorrent.” In re BitTorrent Adult Film Copyright Infringement Cases, 2012 WL 1570765, 1

(E.D.N.Y. 2012). The alleged defendants are identified only by Internet Protocol (IP) addresses, and the plaintiffs may have claims against hundreds to thousands of these defendants at a single time. Id. One media outlet reported that more than 220,000 individuals have been sued since mid-2010 in mass BitTorrent lawsuits, many of them based upon alleged downloading of pornographic works. Jason Koebler, Porn Companies File Mass Piracy Lawsuits: Are You At Risk? U.S. News & World Report (Feb. 2, 2012), <http://www.usnews.com/news/articles/2012/02/02/porn-companies-file-mass-piracy-lawsuits-are-you-at-risk>. In the past five (5) months alone, Plaintiff has filed, in this Court, twenty-six (26) lawsuits implicating four hundred forty-six (446) John Doe Defendants. Each suit claiming defendants downloaded copyrighted pornographic material.

Courts have noted that the risk of inappropriate settlement leverage is enhanced in a case involving salacious and graphic sexual content where a defendant may be urged to resolve a matter at an inflated value to avoid disclosure of the content the defendant was allegedly accessing. Raw Films Inc. v. John Does 1-32, 2011 WL 6840590, 2 (N.D.GA. 2011). In such cases, there is a substantial risk not only of public embarrassment for the misidentified subscriber, but also that the innocent subscriber may be coerced into an unjust settlement with the plaintiff to prevent the public filing of unfounded allegations. Malibu Media, LLC v. John Does 1-5, 2012 WL 2001968, 1 (S.D.N.Y. 2012). The risk of this kind of “shake-down” is compounded when claims involve allegations that a defendant downloaded and distributed sexually explicit, pornographic material. Id. (See e.g., Digital Sin, Inc. v. Does 1-176, 2012 WL 263491, 3 (S.D.N.Y. 2012) (finding that approximately 30% of individuals identified by ISPs in cases against John Doe defendants concerning alleged infringement of adult films are not the individuals who downloaded the films at issue.); Digital Sin, Inc. v. John Does 1-245, 279

F.R.D. 239 (S.D.N.Y. 2012). (determining that “the nature of an alleged copyright infringement of downloading an admittedly pornographic movie, has the potential for forcing coercive settlements, due to the potential for embarrassing the defendants who face the possibility that plaintiff’s thus-far-unsubstantiated and perhaps erroneous allegation will be made public.”).

This case is no exception to the history established by these, so called, “Copyright Trolls.” Plaintiff, Malibu Media, LLC (“Plaintiff”) filed a Complaint on about April 19, 2012 against 22 John Doe defendants alleging copyright infringement. Specifically, the Complaint alleges that the Doe Defendants acted in concert through a peer-to-peer file sharing protocol, known as BitTorrent, to upload, download, and transmit Plaintiff’s property, a pornographic movie named “Tiffany Sex with a Supermodel,” without authorization.

On or about April 24, 2012, Plaintiff filed its Motion for Leave to Serve Third Party Subpoenas Prior to a Rule 26 (f) Conference, as it has done in every other case it filed against the numerous Doe defendants. This Court held a hearing on May 14, 2012 where Plaintiff’s counsel appeared to discuss the Court’s concerns with its April 24, 2012 motion. Defendant argued that it engaged a forensic investigative company named IPP, Limited (“IPP”) to “identify the IP addresses that are being used by those people that are using BitTorrent protocol and the internet to reproduce, distribute, display or perform Plaintiffs’ copyrighted work.” April 10, 2012 Affidavit of Tobias Feiser, Paragraph 12.¹ Based on Plaintiff’s representations, on May 18, 2012, this Court partially granted Plaintiff’s Motion and, subject to the terms of the Order, authorized Plaintiff to serve third party subpoenas prior to the Rule 26 (f) conference. Order, April 24, 2012 (ECF No. 8). However, the Court noted in its May 18, 2012 Order that it was

¹ Interestingly, IPP’s agent, Tobias Feiser, explained that an IP address coupled with the date and time of the questioned activity would allow an ISP to identify the *subscriber*. April 10, 2012 Affidavit of Tobias Feiser, Paragraph 12. However, Mr. Feiser did not suggest that the subscriber information would provide the identity of the actual infringer, a fact that Defendant appears to take for granted.

ruling neither on the “appropriateness of the subpoenas” nor any objections brought by third parties that were not present before the Court. Order, April 24, 2012, ECF No. 8. By letter dated June 13, 2012, Comcast Corporation (“Comcast”) advised Defendant that it would release the requested information on the first business day following July 5, 2012 in the absence of Defendant’s filing a motion to quash the subpoena.²

II. ARGUMENT

A. Defendant has Standing to Challenge the Subpoena and May 18, 2012 Order Because Defendant has a Personal Interest in the Information Subject to the Subpoena.

Generally, a party does not have standing to challenge a subpoena issued to a third party. See Kida v. EcoWater Systems, LLC, 2011 WL 1883194 (E.D.Pa. 2011). However, where the party claims a personal right or privilege regarding the information the subpoena requests, an exception to the rule exists. Id. Here, Plaintiff has alleged that the contact information it seeks will provide identifying information sufficient to name Defendants as copyright infringers and, thereby, seek pecuniary damages. If so, Defendant must have the personal right to object to the disclosure of the information which seeks to subject Defendant to such exposure.

B. The May 18, 2012 Order Granting Permission to Serve Subpoena Should be Vacated and the Subpoena Arising Therefrom Should be Quashed.

The Order granting permission to serve subpoena should be vacated because Defendant’s right to remain anonymous outweighs Plaintiff’s intellectual property rights. The Second Circuit Court of Appeals is the sole federal appellate court to set forth the manner in which an individual’s right to anonymous online speech weighs against another party’s intellectual property rights. See Sony Music Entertainment Inc. v. Does 1-40, 326 F. Supp.2d 556 (S.D.N.Y.

² Although informed by Comcast that Comcast believes moving Defendant is the user of the IP Address identified as John Doe No. 14, this motion is made without any waiver or prejudice to Defendant’s right to dispute that Defendant is the user of the IP address identified as corresponding to John Doe No. 14, which allegations Defendant deny.

2004). The Second Circuit identified five factors that the Court should weigh, which Plaintiff appears to have relied upon in its Motion For leave to Serve Third Party Subpoenas Prior to a Rule 26 (f) Conference:

(1) the concreteness of Plaintiff's showing of a prima facie case of copyright infringement; (2) specificity of the discovery request; (3) absence of alternative means to obtain subpoenaed information; (4) central need for subpoenaed information; and (5) defendants' expectation of privacy.

Id. at 565-66. Instantly, Defendant is insufficiently specific regarding the discovery request and Defendant's expectation of privacy is significant to outweigh any factors in Plaintiff's favor.³

- i. The information requested by Plaintiff is not sufficiently specific to permit the discovery because disclosure will not be likely to lead to the identity of the proper defendants.

The Second Circuit explained that the discovery request must be "sufficiently specific to establish a reasonable likelihood that the discovery request would lead to identifying information that would make possible service upon particular defendants who could be sued in federal court." Id. at 566. In Arista Records LLC v. Doe 3, 604 F.3d 110 (2nd Cir.2010), the Second Circuit was asked to quash a subpoena seeking identification of Doe defendants that the plaintiff alleged had downloaded and/or distributed plaintiff's music in violation of plaintiff's property rights. 604 F.3d at 113. The plaintiff alleged that the defendant infringers accessed the file sharing protocol through a university program and that a total of 236 audio files were present in the file-sharing folder at the time at issue, with at least 6 being songs owned by the plaintiff. The district court, affirmed by the Second Circuit, refused to quash the subpoena.

³ For purposes of this Motion *only*, Defendant concedes that Plaintiff's Complaint and Motion allege sufficient facts to show a prima facie case of copyright infringement, that there is an absence of alternative means to obtain the requested information, and that it has a central need for said information. However, Defendant disputes the veracity of the allegations themselves.

The United States District Court for the Eastern District of New York, like this Court, has been inundated by pornography companies filing suit against Doe defendants and seeking court approval to subpoena identifying information from ISPs. In a nearly identical set of cases, the court granted pre-26(f) conference discovery only with regard to Doe No. 1 in each case, dismissing the claims against all other Does. See In re BitTorrent Adult Film Copyright Infringement Cases, 2012 WL 1570765 (E.D.N.Y. 2012). The court determined that the discovery requests, while sufficiently specific in detail, did not “establish a reasonable likelihood” that the information yielded would “lead to the identity of defendants who could be sued.” Id. at 13. The court stated that “the assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time.” Id. In fact “it is no more likely that the subscriber to an IP address carried out a particular computer function . . . than to say an individual who pays the telephone bill made a specific telephone call.” Id.⁴

The BitTorrent court differentiated its case from Arista Records in that the ISP involved in Arista Records was located at a university and, therefore, it was likely that the end user was a particular individual, not a wireless network. Id. at 14. Further, the court found it significant that the file folder at issue in Arista Record contained more than 200 songs, where the BitTorrent Doe defendants were alleged to have infringed on a single video. Id.

The instant matter is identical to those addressed in BitTorrent. Defendant is accused of infringing on one work owned by Plaintiff, but there is no indication that, even if Plaintiff received identifying information about the subscriber, Plaintiff would be unable to assert that the

⁴ Interestingly, while Plaintiff refuses to do so here, at least one similar Plaintiff conceded that “in some cases ‘the Subscriber and the Doe Defendant [will] *most likely not [be] the same individual.*” Pac. Century Int’l Ltd. v. Does, 2011 WL 5117424, 2 (N.D. Cal. Oct. 27, 2011) motion to certify appeal denied, C-11-2533-DMR, 2011 WL 5573952 (N.D. Cal. Nov. 15, 2011). Also See Digital Sin, Inc. v. John Does 1-176, 279 F.R.D. 239 (S.D.N.Y. 2012).

subscriber is the individual who performed the alleged infringing action. It is noteworthy that Plaintiff's affiant states, not that the IP address will lead Plaintiff to the infringer, but merely to the "subscriber." April 10, 2012 Affidavit of Tobias Feiser, Paragraph 9. As in BitTorrent, there is utterly no indication that, here, the subscriber is the individual who committed the acts alleged by Plaintiff. Plaintiff has not alleged anything more than that its property was downloaded and/or distributed by certain IP addresses, allegations which are insufficient to support Plaintiff's request for pre-26(f) conference discovery.

- ii. Defendant's Expectation of Privacy in his identifying information outweighs disclosure where Plaintiff has not sufficiently shown that Defendant infringed on Plaintiff's property.

It has been concretely established that, while anonymous speech is protected, it is not sheltered when used to infringe on another's copyright. Arista Records, 604 F.3d at 118. Additionally, the Sony Music court explained that an infringing defendant is entitled to "little expectation of privacy" when committing the infringing act. Sony Music, 326 F. Supp. 2d at 566-67. The BitTorrent court, understanding that the subscriber cannot be presumed to be the infringer, however, refused to minimize the Does' expectation of privacy.

Instantly, Plaintiff has minimal support for its allegations that Defendant, even if identified as the subscriber, would be a proper Doe defendant here. In fact, it is often more likely that the subscriber is not the infringer. It follows that it would be improper to find Defendant's expectation of privacy abrogated where there is such a high likelihood that Defendant is not the individual who committed the alleged infringing conduct.

- iii. Prior Orders of this Court failed to take into account the unreliability of the IP address in locating the proper Doe defendant.

Defendant acknowledges that the Honorable Mary A. McLaughlin, of this Court, issued a Memorandum Decision on March 23, 2012 substantially in contravention with Defendant's

arguments herein. See Raw Films, Ltd. v. John Does 1-15, Docket No. 11-7248, Order, March 23, 2012. Judge McLaughlin explained that the Court took into account the fact that the subscriber may not turn out to be alleged infringer, but that the “Rules permit parties to obtain discovery of ‘the identity and location of persons who know of any discoverable matter.’” Raw Films, Ltd. v. John Does 1-15, Docket No. 11-7248, Order, March 23, 2012, n. 3 citing, in part, to Red. R. Civ. P. 26 (b)(1). Instantly, Plaintiff has made no assertion that Defendant is an individual with knowledge of who, in the event the subscriber is not the infringer, may have infringed upon Plaintiff’s property rights. Plaintiff maintains, in spite of its obvious unreliability, that the IP address itself will provide the identity of the proper defendants. This is a leap that Plaintiff simply cannot make.

C. In the event this Honorable Court denies Defendant’s request to vacate its May 18, 2012 Order and quash the subpoena, a Protective Order should be issued so that Plaintiff may not publicly disclose Defendant’s information and identity.

Federal Rule of Civil Procedure 26 authorizes this Court to enter a protective order in order to “protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including . . . specifying terms . . . for the disclosure or discovery . . . or limiting the scope of disclosure or discovery in certain matters.” Fed.R.C.P. 26 (c)(1)(B) & (D).

Instantly, the failure to enter a protective order will result in the disclosure of Defendant’s identity associated with the alleged improper download and sharing of pornographic materials; an accusation which would cause embarrassment and injury to Defendant’s reputation. Frequently, as some plaintiffs have admitted, the identified subscriber is often not the appropriate Doe defendant. Unfortunately, even after Defendant is able to prove that Plaintiff’s allegations are false, the stain of the accusation will not be removed from Defendant’s character.

A protective order should be entered, at a minimum, prohibiting the public disclosure of any information relating to Defendant obtained via the subpoena. In addition, the protective order should require that all court filings, in this action, containing or referencing information related to Defendant obtained via the subpoena, must be filed under seal or redacted in order to avoid the public disclosure of Defendant's confidential information.

The entry of a protective order would alleviate, to some extent, the concern that Plaintiff has filed this action, and numerous other actions, in order to harass and embarrass a settlement out of Defendants. Multiple courts faced with identical situations have expressed concern that Plaintiff, and its pornography-industry colleagues, have filed suits against Doe defendants with the express intent of coercing settlements out of defendants who may, or may not, have been involved in the alleged conduct. See In re BitTorrent Adult Film Copyright Infringement Cases, 2012 WL 1570765 (E.D.N.Y. 2012). Precluding the public disclosure of Defendant's identity would lessen *some* of the concern that Defendant's involvement in this action is merely to extort a financial gain for Plaintiff, rather than actually protecting its property interests.⁵

In the event this Honorable Court does not vacate its Order and quash the Subpoena, the Court should, alternatively, enter a protective order which: (1) prohibits the public disclosure of any information relating to Defendant that is obtained as a result of Plaintiff's subpoena; and (2) require that any party filing any pleading or document, which contains references to Defendant's confidential information obtained via the subpoena, in the instant action redact said information or file the pleading or document under seal.

⁵ Defendant does not contend that a protective order is sufficient to completely placate the concerns. Merely being involved in this case, without good cause, is enough to serve as harassing and cause unnecessary embarrassment and undue burden. However, if Plaintiff is required to keep Defendant's information and identity completely confidential, it may decrease the likelihood that Defendant's reputation is irreversibly damaged by Plaintiff's false and malicious allegations.

III. CONCLUSION

For all of the reasons stated herein, Defendant respectfully requests that the Court grant Defendant's Motion in the form of the Order attached hereto.

Respectfully Submitted

LEISAWITZ HELLER ABRAMOWITZ PHILLIPS, P.C.

Dated: 7/5/12

BY:



Thad M. Gelsinger, Esquire

Attorney I.D. No. 208233

Telephone: (610) 372-3500

Facsimile: (610) 372-8671

tgelsinger@LeisawitzHeller.com

Attorneys for Defendant, John Doe No. 14