IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Malibu Media, LLC Plaintiff, v. John Does 1-16, Defendants.	Civil Action No. 1:12-cv-00840-PAB-MEH FILED UNITED STATES DISTRICT COURT DENVER, COLORADO MAY 25 2012 GREGORY C. LANGHAM CLERK

JOHN DOE'S (IP ADDRESS 98.245.57.194) MOTION TO DISMISS AND/OR ISSUE A PROTECTIVE ORDER, AND INCORPORATED MEMORANDUM OF LAW

Comes now, **John Doe #10, I identified by the IP address 98.245.57.194**, file this Motion and moves this Court to: dismiss and/or issue a protective order in connection with the subpoena (the "Subpoena") directed at Comcast and objects to the discovery sought.

The case against JOHN DOES 1-16 is a strategic campaign by Plaintiff to coerce innocent people to settle out of court for exorbitant amounts to avoid embarrassment due to the association with Plaintiff's products (ie pornography). This tactic imposes an unfair cost and burden on numerous innocent defendants, a fact plaintiff uses to its advantage, to obtain unscrupulous settlements. The Plaintiff in this case has instituted a lucrative procedure at the taxpayers' expense where it initiates legal proceedings based on questionable allegations, against anonymous defendants, in hopes of extracting quick settlements. Similar plaintiffs have tiled thousands of similar "John Doe suits" across the county. *See, e.g., Parrick Collins Inc., K-Beech Inc, Raw Films Ltd., Diabolic Video Productions Inc., v. Does 1-1.544* in the 11th Judicial Circuit for Miami-Dade County, Florida, Case No. 11-24714 CA 22. The Defendant asks this Court to (1) dismiss the action against the Defendant and quash the subpoena

seeking the personal information of the Defendant, or in the alternative, grant a protective order preventing the disclosure of any information obtained through a subpoena.

PROCEDURAL HISTORY

On May 1, 2012, an order was entered by this Court on Plaintiff Malibu Media, LLC's ("Malibu Media") unopposed motion, which allowed Plaintiff to serve subpoenas on the Internet Service Providers ("ISP") of the 16 defendants. Defendant was notified of this matter through Comcast, the Defendant's ISP. The Defendant was informed by Comcast that its personal information had been subpoenaed by Plaintiff.

JOHN DOE(IP 98.244.57.194) DECLARES AS FOLLOWS:

1. Bit Torrent is one of the most common peer-to-peer file sharing protocols used for distributing large amounts of data; indeed, it has been estimated that users using the Bit Torrent protocol on the internet account for over a quarter of all internet traffic. The creators and users of Bit Torrent developed their own lexicon for use when talking about Bit Torrent, which can be found on www.Wikipedia.org.

2. The Bit Torrent protocol's popularity stems from its ability to distribute a large file without creating a heavy load on the source computer and network. In short, to reduce the load on the source computer, rather than downloading a file from a single source computer (one computer directly connected to another), the Bit Torrent protocol allows users to join a "swarm" of host computers to download and upload from each other simultaneously (one computer connected to numerous computers).

3. Plaintiffs fail to sufficiently identify defendants by IP address. Plaintiff asserts that Defendant,

identified only by IP address, was the individual who accessed the Work. The assumption that the person who pays for internet access at a given location is the same individual that allegedly downloaded a specific movie has grown tenuous over time. An IP address provides only the location at which one of any number of computer devises may be deployed; much like a telephone number can be used for any number of telephones. Thus, it is no more likely that the subscriber of an IP address carried out a particular computer function, such as downloading a movie, than to say an individual who pays the telephone bill made a specific telephone call. Today, a vast majority of households, including that of the Defendant, use a wireless router as part of their internet service. In regards to wireless routers, a single IP address supports multiple devices, which can be operated simultaneously by different individuals. In the case of someone using an unsecured wireless router, an outside party can access their internet connection. This outside party can surf the internet, send email, upload files, or download content. This unknown outside party would have the same IP Address as anyone on the router itself. Therefore, there is no way to know, reliably and accurately, who the offending party was. Due to these circumstances, there is no telling who could have performed the alleged download, whether it is a family member, a visitor, or a complete stranger. Further, unless the wireless router has been secured through an appropriate channel, and even then it may not be completely secure, neighbors or any random stranger can access the internet using the IP address assigned to the Defendant. The court in *Latham* stated that, "the only way to prevent sharing of the wireless router is to encrypt the signal and even then an individual can bypass this security using publicly available software. As a result, the Plaintiff has a very difficult job of identifying a defendant with any certainty. The Plaintiff should not be allowed to impose monstrous expense and burden on 16 people to disprove their case, when the foundation of their allegations is unreliable. Clearly, the burden of proof in this case rests on the Plaintiff. Due to the current state of wireless internet access, serious doubt is cast on Plaintiff's

assertions that the "ISP to which each Defendant subscribes can correlate the Defendant's IP address to the Defendant's true identity." The Court in *Digital Sin, inc. v. Does i-i76* 2012 WL 263491 (S.D.N.Y. Jan. 30, 2012), stated it was "'concerned with the possibility that many of the names and addresses produced in response to the plaintiff's discovery request will not in fact be those of the individuals who downloaded the movie in question." The court further noted that "the risk of false positives gives rise to the potential for coercing unjust settlements from innocent defendants such as individuals who want to avoid the embarrassment of having their names publicly associated with allegations of illegally downloading obscene movies." Although the Complaint states that IP addresses are assigned to devices and thus by discovering the individual associated with the IP address the true identity of the defendants will be revealed, this is unlikely the case. Most, if not all, the IP addresses will reflect a wireless router or some type of networking device. Thus, while the ISP's will provide the name of its subscriber, the alleged infringer might not be the subscriber at all, but a member of their family, a guest, a stranger, a neighbor, or an internet thief.

4. The subpoena must be quashed. Or at a minimum, a protective order should be issued. Based on the above, Defendant requests that the subpoena issued to its ISP, Comcast, be quashed by dismissing Defendant from this suit due to Plaintiffs failure to prove the Defendant accessed the Work via the reported IP address. Such a request would be consistent with the trend of courts throughout the nation, all of which have quashed subpoenas issued by similar litigants due to similar issues. *See Digiprotect USA Corp. v. Does 1-266,* No. 10 Civ. 8759 (S.D.N.Y. 201 J); *Raw Films, Ltd., v. John Does 1-32,* No. 3:11CV532 (E.D. Va. Oct. 5, 2011); and *Diabolic Video Productions, Inc. v. Does 1-2099,* No. 10-CV-5865-PSG (N.D. Cal. 2010).

FRCP Rule 26(c) allows upon moving the court and for good cause shown, the court may take any order to protect a party or person from issuing an order to protect a party or person from annoyance,

embarrassment, oppression, or undue burden. The Court is given broad discretion to prohibit or limit discovery and is reviewed on an abuse of discretion standard. If Defendant is named relating to sharing pornographic films, embarrassment and damage to Defendant's reputation is assured. No matter what transpires in the future, Plaintiff knows the potential embarrassment is enough to coerce a settlement and hence these cases are pursued. At the minimum, Defendant requests any identifying information remain sealed and confidential, or that the Court issue some form of protective order to prevent embarrassment, oppression, and annoyance as justice may so require.

CONCLUSION

Plaintiff has demonstrated that it is far more interested in obtaining ISP subscribers' contact information for use in extracting large settlements than the formalities of the legal process and privacy interests of the affected individuals. On May 8, 2012, a local Denver news station, Channel 7, conducted an investigation regarding these cases being brought in Colorado and into Mr. Kotzker's tactics. The report states that Mr. Kotzker has filed cases against approximately 800 John Does over the past seven months. The report can be found here, http://www.thedenverchannel.com/news/31030100/detail.html.

My hope is that this Court will see through Mr. Kotzker's practices as being nothing more than a strategy of coercion, harassment and use of embarrassment associated with the porn industry. If this action is allowed to proceed forward, many thousands of the countless millions of internet users, or other "defendants" will be dragged into lawsuits such as these, simply to use the same '"embarrassment" tactics to extract money from legally unknowledgeable people, "guilty" or not.

Therefore, premises, considered, John Doe respectfully requests that this Court:

(a) Issue a protective order prohibiting the ISP WOW from disclosing any of John Doe's personally identifying information;

(b) Order that any party seeking to file with the Court any of John Doe's confidential and personally identifiable information obtained from Comcast in response to Plaintiff's May 1, 2012 Subpoena shall make such a filing as a Restricted Document with an accompanying Motion to Restrict Access.

(c) Provide any further relief to Defendant that is just and proper.

Respectfully submitted,

Under penalty of perjury, I declare that the foregoing facts are true and correct.

Date : May 24, 2012

John Doe #10.

JOHN DOE #10 (IP 98.244.57.194)

jean_ch@hanmail.net