RECEIVED
AUG 22 2012
AT 8:30 M
WILLIAM T. WALSH, CLERK

IN THE UNITED STATES DISTRICT
FOR THE DISTRICT OF NEW JERSEY

MALIBU MEDIA, LLC.

Plaintiff,

v.

JOHN DOES 1-30,

Defendants.

Civil Action No. 3:12-cv-03896-JAP-DEA

MOTION TO QUASH OR MODIFY SUBPEONA

MOTION TO DISMISS AND/OR SEVER COMPLAINT AGAINST DEFENDANT JOHN DOE 22 AND QUASH SUBPOENA AGAINST SAME

I, John Doe #22 (hereinafter "Defendant"), respectfully motion the court to allow Defendant to proceed anonymously and for dismissal or severance of my case in the above captioned matter and to quash the subpoena served on my Internet Service Provider ("ISP"), Cablevision Systems Corporation.

FACTUAL BACKGROUND

1. On July 03, 2012, this Court issued an Order permitting Plaintiff to serve a Rule 45 subpoena on each Defendant's internet service provider seeking personally identifying information about each Defendant, including Defendant's name, physical address, telephone number, e-mail address, and media access control ("MAC") address.

2. On July 06, 2012, Defendant's ISP was served with a subpoena issued from the United States District Court for the District of Eastern New York and served in Bethpage, NY, that demanded Cablevision to produce to Plaintiff at Plaintiff's counsel's office in Flemington, NJ, the

personally identifying information regarding Defendant in connection with Plaintiff's claim that Defendant allegedly unlawfully downloaded a film allegedly owned by Plaintiffs ("work").

3. The ISP provided written notice to Defendant on August 1, 2012 via UPS delivery.

4. The ISP's letter stated that Cablevision would provide the requested information to Plaintiff by August 24, 2012. The ISP's letter further advised Defendant that if Defendant had any objections to the subpoena, Defendant needed to file those objections with the Court prior to August 24, 2012.

INTRODUCTION

I, the Defendant, have never committed the act alleged by the Plaintiff, nor have access to given that I was working abroad during the dates of the alleged infringement April 12, 2012. Nor should I be found liable for the use of unsanctioned wireless router activity during my absence.

Upon researching into Malibu Media, LLC, I have found that when subpoenaed information is turned over to the Plaintiff, the Defendants, guilty or innocent, are pressured to settle the issue for thousands of dollars to avoid dealing with threatened lawsuits. These demand letters and the subsequent telephone calls, which have been reported as persistent if not harassing are the core of the Plaintiff's business model. As Magistrate Judge Gary R. Brown submitted in his Order & Report & Recommendation (ORR) in the United States District Court for the Eastern District of New York – ***K-Beech, Inc. v. John Does 1-37***, No. 2:11-cv-03995 (D. NY. May 01, 2012) Doc #39.

> Plaintiffs clearly need identification of the putative John Does in order to serve process on them and prosecute their claims. However, not all the information sought is required to advance the claim. For example, in addition to names and addresses, plaintiffs seek both the home telephone numbers and email addresses of the putative John Does, *see Malibu 26,* Proposed Order DE [3-2], information which is clearly not required to proceed with this action. In

> particular, obtaining the home telephone numbers seems calculated to further plaintiffs' settlement strategies, discussed above, rather than advancing their claims by allowing them to effect service.

Plaintiff again seeks to take advantage of the threat of an award of statutory damages, attorneys' fees, ignorance about copyright law, and the stigma associated with accessing pornography via the internet to extract quick and profitable settlements. Other courts have specifically and directly condemned for-profit copyright litigation models against individuals. *Righthaven, L.L.C. v. Hill*, No. 1:11-cv-00211 (D. Colo. Apr. 7, 2011) (J. Kane), Dkt. 16 ("Plaintiff's wishes to the contrary, the courts are not merely tools for encouraging and exacting settlements from Defendants cowed by the potential costs of litigation and liability.") Although Plaintiff does not rely on the same business model as the Righthaven model, Plaintiff does seek to exact settlements from numerous Defendants sued in a John Doe capacity in an amount to which mounting a defense in Court is less economically efficient than settling out of court.

The Plaintiff's argument for Joinder also is refuted by the alleged infringement dates of the mentioned Defendants. As the Plaintiff states:

> Pursuant to Fed. R. Civ. P. 20(a)(2), each of the Defendants was properly joined because, as set forth in more detail below, Plaintiff asserts that: (a) each of the Defendants is jointly and severally liable for the infringing activities of each of the other Defendants, and (b) the infringement complained of herein by each of the Defendants was part of the same series of transactions, involving the exact same piece of Plaintiff's copyrighted Work, and was accomplished by the Defendants acting in concert with each other…

However, with the Defendant's limited understanding of peer-to-peer file sharing protocols, the Defendant assumes that to prove any "Defendants acting in concert with each other" would require the infringements to occur on the same day. Rather this improper joinder fits into the aforementioned business model to avoid the cost of appropriately filing individual cases against

each John Doe Defendant as this same Plaintiff with the same attorney currently has a dozen related cases in the United States District Court for the District of New Jersey:

> Plaintiff's subpoena is also invalid on its face as stated under 'Parties,' "4. The ISP to which each Defendant subscribes can correlate the Defendant's IP address to the Defendant's true identity." This reliance on IP address has been proven as unsubstantial in numerous similar cases and again addressed by Magistrate Judge Gary R. Brown – *K-Beech, Inc. v. John Does 1-37*, No. 2:11-cv-03995 (D. NY. May 01, 2012) Doc #39.

> In sum, although the complaints state that IP addresses are assigned to "devices" and thus by discovering the individual associated with that IP address will reveal "defendants' true identity," this is unlikely to be the case. Most, if not all, of the IP addresses will actually reflect a wireless router or other networking device, meaning that while the ISPs will provide the name of its subscriber, the alleged infringer could be the subscriber, a member of his or her family, an employee, invitee, neighbor or interloper.

Furthermore, negligence claims due to the actions of others using a subscriber's IP address have been argued against in an *Amicus Curiae* by the Electronic Frontier Foundation (EFF) in *Liberty Media Holdings, LLC v. Cary Tabora and Schuyler Whetstone*, No. 1:12-cv-02234(D. NY March 27, 2012) resulting in Dismissal Order by District Judge Lewis A. Kaplan Doc# 33.

> Liberty nevertheless argues that its negligence claim asserted here17 is not preempted because, as the Court understands the argument, the negligence claim rests on infringement by others whereas the Copyright Act provides a remedy only against a direct infringer.18 In light of the preceding discussion and the doctrine of contributory infringement – which Liberty's memorandum ignores entirely – that position is untenable.

Therefore, since the Plaintiff's goal is to obtain information about the Defendant in order to potentially exact a settlement, the Defendant Motions for Leave to Proceed Anonymously. Given that the Defendant was working overseas during the alleged infringement and thus could

not be the alleged infringer and given the wrongful joinder of these 30 John Does with unsubstantial collusion evidence, the Defendant motions to sever or dismiss this Defendant from this case. Lastly, as the Plaintiff's purpose for obtaining true identities of Defendants is to potentially force a settlement by threatening embarrassing public naming of this Defendant, Defendant motions to quash the subpoena to ISP disclosing Defendant's information or to limit information to only name and address.

ARGUMENT

I. DEFENDANT SHOULD BE ALLOWED TO PROCEED ANONYMOUSLY.

As an initial matter, Defendant respectfully requests that he be permitted to proceed anonymously in filing this motion. Proceeding anonymously is the only method of not rendering moot these proceedings by disclosing the very same information which Plaintiff seeks to obtain through its improper subpoena. In other words, quashing the subpoena while requiring Defendant to proceed in hs own name would entirely defeat the purpose of the motion to quash. Accordingly, Defendant respectfully requests that the Court permit him to proceed anonymously.

II. PLAINTIFF'S SUBPOENA SHOULD BE SEVERED OR DISMISSED DUE TO IMPROPER JOINDER

1. **Financial Reasoning to Improper Joinder**

To minimize court costs while suing or threatening to sue as many individuals as possible, Plaintiff's counsel, Patrick J. Cerillo, Esq, is using improper joinders as been typical in Malibu Media, LLC suits alleging copyright infringement through BitTorrent. Information retrieved from PACER (http://www.pacer.gov/) indicates that Mr. Cerillo filed 3 lawsuits on behalf of Malibu Media, LLC in the New Jersey District Court on June 26, 2012. An additional 2 filings on behalf of Malibu Media, LLC were made on July 26, 2012 and 1 on August 13, 2012 and 2 on August 14, 2012 and a further 2 on August 15, 2012. Altogether, these 10 Malibu Media, LLC lawsuits involve 307 defendants and have been assigned to 8 different judges in the same district Court with 8 different referred magistrate judges. The individual lawsuits have from 12 to 81 defendants each, averaging 30. Thus far in 2012, Malibu Media LLC has filed more than 130 suits in California, Colorado, the District of Columbia, Florida, Maryland, New York, Pennsylvania, Texas and Virginia against numbered Does using similar tactics. These suits collectively name almost 2200 defendants, averaging almost 17 per case.

Federal courts have previously recognized this improperness of joinder. In a BitTorrent case nearly identical to this one, *CP Productions, Inc.* v. *Does 1-300* case 1:201 Ocv06255, the court noted before dismissal:

> [I]f the 300 unnamed defendants have in fact infringed any copyrights (something that this court will assume to be the case, given the Complaint's allegations that so state), each of those infringements was separate and apart from the others. No predicate has been shown for thus combining 300 separate actions on the cheap -if CP had sued the 300 claimed infringers separately for their discrete infringements, the filing fees alone would have aggregated $105,000 rather than $350.

In the same vein, in the Southern District of New York, Judge Colleen McMahon wrote when dismissing all but one of the defendants (John Doe #1) in *Digital Sins, Inc. vs. John Does J*-245

Caye J:JJ-cv-08J7()"cM, "They are dismissed because the plaintiff has not paid the filing fee that is statutorily required to bring these 244 separate lawsuits." In that case the underpayment exceeded $85,000.00.

Commenting on the same case, Judge Milton Shadur wrote:

> This Court has received still another motion by a "Doe" defendant to quash a subpoena in this ill-considered lawsuit filed by CP Productions, Inc. ("CP") against no fewer than 300 unidentified "Doe" defendants -this one seeking the nullification of a February 11, 2011 subpoena issued to Comcast Communications, LLC. This Court's February 24, 2011 memorandum opinion and order has already sounded the death knell for this action, which has abused the litigation system in more than one way. But because the aggrieved Doe defendants continue to come out of the woodwork with motions to quash, indicating an unawareness of this Court's dismissal of this action, 1 CP's counsel is ordered to appear in court on March 9, 2011 at 9:00 a.m. Counsel will be expected to discuss what steps should be taken to apprise all of the targeted "Doe" defendants that they will not be subject to any further trouble or expense as a result of this ill-fated (as well as ill-considered) lawsuit.

2. **Date & Bit Torrent Reasoning to Improper Joinder**

U.S. District Judge Murray Snow for the District Court for the District of Arizona held in a matter on March 19, 2012 that in order to be sued with other John Doe Defendants in Bit Torrent download cases, the individual must have either uploaded or downloaded from the other defendants in order for the first element to be met.

> Plaintiff alleges that the two remaining Defendants "participat[ed] in the BitTorrent swarm with other infringers" but does not claim that John Doe 6 provided data to the former John Doe 12 or vice versa. (Doc. 26 ¶ 56)… Plaintiff has not demonstrated that John Doe 6 and the former John Doe 1`2 engaged in a single transaction or occurrence, or a single series of transactions or occurrences.

Defendant John Doe 6 has been improperly joined, and is severed from the lawsuit. *Patrick Collins, Inc. v. John Does 1-54* (Case No. 2:12-cv-01602).

Despite Plaintiff's claims to the contrary, the Defendants 1-30 herein did not participate in the same transaction or occurrence, the same series of transactions or occurrences as required by the joinder; nor, did they act in concert with one another. To the contrary, Plaintiff's own exhibit attached to the Complaint indicates that downloading occurred at different times and dates within a six week range between March 02, 2012 and June 08, 2012, an almost twelve week period wherein the Plaintiffs allege that Defendants were acting in concert. None of the other John Does named to the lawsuit are alleged to have accessed the swarm or the Bit Torrent tracker on or near the April 12, 2012 date alleged by Plaintiff. Plaintiff has not demonstrated in any way that this Defendant's IP address was used to access the alleged Bit Torrent tracker at the same time and transaction as the other Defendants nor have they demonstrated for how long Defendant's IP address was used to access the files if at all.

3. **Unsubstantiated User of IP Reasoning for Dismissal**

An ISP may keep records of a particular MAC address to access an specific IP address, but that MAC address could be a wireless router (as is the case with Defendant) thus obfuscating what end devices actually connect via that IP address. If, as may often be the case, it is not possible to identify the device used to access the internet, much less the person operating the device, simply classifying all persons to whom implicated IP addresses are registered as offenders creates a significant possibility, even probability if repeated often enough, that a number of persons who have done no wrong will be served and possibly elect to settle claims out of court as an expedient. For some this may be a simple business decision: it will cost less to settle than to litigate; for others who lack the financial resources to mount an adequate defense, the "choice" is forced upon them. This creates the potential for a coercive and unjust settlement and this has also been recognized by the courts in various jurisdictions. The Magistrate Judge Gary R. Brown writing on ***K-Beech, Inc. v. John Does 1-37***, No. 2:11-cv-03995 (D. NY. May 01, 2012) Doc #39 when evaluating the potential for coerced settlements noted that:

Many courts evaluating similar cases have shared this concern. *See, e.g., Pacific Century Int'l, Ltd* v. *Does* 1-37-F. Supp. 2d--, 2012 WL 26349, at *3 (N.D. IlL Mar. 30,2012) ("the subscribers, often embarrassed about the prospect of being named in a suit involving pornographic movies settle"); *Digital Sin, 2012* WL 263491, at 3 * ("This concern and its potential impact on social and economic relationships, could impel a defendant entirely innocent of the alleged conduct to enter into an extortionate settlement") *SBO Pictures,* 2011 WL 6002620, at *3 (defendants, whether guilty of copyright infringement or not would then have to decide whether to pay money to retain legal assistance that he or she illegally downloaded sexually explicit materials, or pay the money demanded. This creates great potential for a coercive and unjust 'settlement'"). [po 18]

In *Case 2:11-cv-03995* which addressed three cases *(Malibu Media, LLC v. John Does* 1-26, *CV 12-1147 (J..)) (GRB). lvlalibu Media, LLC v. John Does 1-1I,* C'V *12-1I50 (LDW) (GRB),* and *Patrick Collins, 1nc. v. John Does* 1-9, *CV 12-1154 (ADS) (GRB))* U.S. Magistrate Judge Gary Brown in discussing these issues noted that:

'" These developments cast doubt on plaintiff's assertions that "[t]he ISP to which each Defendant subscribes can correlate the Defendant's IP address to the Defendant's true identity." *See, e.g., Alalibu* 26, CompL At ~9, or that subscribers to the IP addresses listed were actually the individuals who carried out the complained of acts. *As* one judge observed:

> The Court is concerned about the possibility that many of the names and addresses produced in response to Plaintiff's discovery request will not in fact be those of the individuals who downloaded "My Little Panties # 2." The risk is not purely speculative; Plaintiff's counsel estimated that 30% of the names turned over by ISPs are not those of individuals who actually downloaded or shared copyrighted material. Counsel stated that the true offender is often "the "teenaged son ... or the boyfriend if it's a lady." Alternatively, the perpetrator might tum out to be a neighbor in an apartment building that uses shared IP addresses or a dormitory that uses

> shared wireless networks. 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 "My Little Panties # 2" [pps. 7 -8, citations omitted in the original, emphasis original].

Judge Brown also observed that another judge had previously noted [citations omitted in the original]:

> the ISP subscriber to whom a certain IP address was assigned may not be the same person who used the Internet connection for illicit purposes... By defining Doe Defendants as ISP subscribers who were assigned certain IP addresses, instead of the actual Internet users who allegedly engaged in infringing activity, Plaintiff's sought-after discovery has the potential to draw numerous internet users into the litigation, placing a burden upon them that weighs against allowing the discovery as designed. [ibid, p. 81

Finally, also writing in case 2: *ll-cv-03995,* Judge Brown described the litigation practices in cases where pre-service discovery is the basis for identifying putative defendants as "abusive" and went on to state:

> Our federal court system provides litigants with some of the tiniest tools available to assist in resolving disputes; the courts should not, however, permit those tools to be used as a bludgeon. As one court advised Patrick Collins Inc. in an earlier case, "while the courts favor settlements, filing one mass action in order to identify hundreds of doe defendants through pre-service discovery and facilitate mass settlement, is not what the joinder rules were established for." Patrick Collins, Inc. v. Does 1-3757,2011 U.S. Dist. LEXIS 128029, at *6-7 (N.D.Cal. Nov. 4, 2011).

Given that this Defendant was working overseas during the alleged infringement, the infringer is someone else who accessed the internet via the Defendant's wireless router or some other means. To name this Defendant in any subsequent filings would be tantamount to a

negligence claim to which Judge Lewis A. Kaplan dismissed in *Liberty Media Holdings, LLC v. Cary Tabora and Schuyler Whetstone*, No. 1:12-cv-02234(D. NY March 27, 2012) Doc# 33.

Plaintiff fails to show that the claims against each Doe Defendant arose out of the same transaction, occurrence, or series of transactions or occurrences, and therefore, Defendants must be severed and/or dismissed.

III. PLAINTIFF'S SUBPOENA MUST BE QUASHED

1. Plaintiff's Subpoena Must be Quashed on the Basis of the Lack of Reliability relating to IP Address and MAC Address Tracking Technology

Plaintiff's subpoena must be quashed because the technology used to identify individual Defendants for the alleged copyright infringement is unreliable and is insufficient to show a volitional act of copyright infringement. Specifically, there is not only software available that is capable of impersonating and/or falsifying an IP address, but such software is unreliable because the software does not also identify the associated computer's MAC address at the time.

Because IP addresses are the **only** evidence Plaintiff has to identify Doe Defendants, Plaintiff's subpoena is unreliable on its face and should be quashed by the Court given the evidence Plaintiff has provided thus far. Moreover, to prove a claim for infringement, a Plaintiff must demonstrate that the Defendant copied the protected work. *Kelly v. Ariba Soft Corp.*, 336 F.3d 811, 817 (9th Cir. 2003) ("the Plaintiff must show ownership of the copyright and copying by the Defendant."), and that the copying was a result of a volitional act. *See Religious Tech Ctr. v. Netcom On-Line Commn'n Servs., Inc.,* 907 F. Supp 1361, 1369-1370 (N.D. Cal. 1995). However, Plaintiff's allegations are highly suspect and do not, and cannot account for numerous issues, including unsecured wireless networks, fraudulently broadcasted IP addresses, computer hacking, and more.

Moreover, Plaintiff also has the ability to pursue the Defendants in a much less intrusive manner than their current dragnet approach. Prospective Plaintiffs can file through the various ISPs notices of infringement, wherein the ISP relays via email the notice of infringement to the prospective Defendant. Plaintiffs can then attempt to settle with Defendants in a manner less expensive for all parties. If the potential Defendants fail to comply with Plaintiffs requests for settlement, Plaintiffs can then choose to sue the individuals who fail to comply. This method employed by other copyright enforcement groups creates much less of a dragnet, allows potential Defendants to remain anonymous, reduces costs to all parties, preserves precious judicial resources, and allows Plaintiffs to more efficiently identify Defendants and settle without resorting to numerous Federal lawsuits.

In the present circumstances, Defendant was not in New Jersey at the time that the allegedly infringement and thus in this case it is evident that the Defendant is not the infringer. There is an alternative method of copyright enforcement that Plaintiff could utilize which is less expensive than the current means relied on by Plaintiff's broad sweeping approach. Coupled with the devastating effect of a false accusation of infringement of pornographic materials, Plaintiff's allegations fail to provide sufficient accuracy, nor an actual volitional act associated to a Defendant sufficient to support its claim, and Plaintiff's subpoena should be quashed.

2. The Subpoena Should be Quashed to Protect Defendant from Unreasonable Annoyance and Public Embarrassment

The Court must quash the present subpoena against John Doe #22 to prevent Defendant from suffering unwarranted annoyance, embarrassment, and an undue burden. Fed. R. Civ. Pro. 45(c)(3)(A)(iv). Presently, Plaintiff requires Defendant's confidential personally identifying information from Defendant's ISP so that Plaintiff can harass Defendant into coercing a quick

and profitable settlement under the guise of publicly outing Defendant regarding an accusation of an unlawful download of pornographic material, despite questionable proof against Defendant. Plaintiff's subpoena is intended to cause an undue annoyance, embarrassment, and hardship to Defendant, and the same would result if Defendant's personally identifying information were associated without sufficient evidentiary support with the unlawful downloading of pornographic materials. Such association would be highly embarrassing to Defendant, unjustifiably stigmatizing to Defendant, injurious of Defendant's character and reputation as a New Jersey state resident, and potentially jeopardizing to Defendant's employment. If the Plaintiff only wanted to engage in justifiable practices, there would be no need for them to request telephone numbers and email addresses for a name and physical address should suffice in delivering relevant documents.

Moreover, even after Defendant demonstrates that Plaintiff's allegations are false, the embarrassment and reputational damage from Plaintiff's false public claim will persist because of the public record. However, by quashing Plaintiff's subpoena, the Court can prevent the injustice of having Defendant unjustly harmed and embarrassed by questionable and premature accusations of illegally downloading pornographic materials. Given the present facts, the subpoena should be quashed or at least modified to allow ISP to disclose only name and address.

Respectfully Submitted,

Dated: 8/15/2012

J Doe

John Doe #22, IP Address 69.126.229.98

Pro Se

CERTIFICATE OF SERVICE

I hereby certify that on Aug. 22, 2012, a true and correct copy of Motion to Dismiss and/or Sever Against John Doe 14 and Quash Subpoena Against Same by United States first class mail to:

Patrick J. Cerillo, Esq.
Patrick J. Cerillo, LLC.
4 Walter Foran Boulevard
Suite 402
Flemington, NJ 08822

Date: 8/15/12

John Doe #22, IP Address 69.126.229.98

Pro Se

Clerk's Office

United States District Court for the District of New Jersey

RE: Malibu Media, LLC v. Does 1-30

Case No.: 3:12-cv-03896-JAP-DEA

IP Address: 69.126.229.98

Dear Sir/Madam,

I am one of the defendants in the above referenced matter. My IP address is 69.126.229.98 John Doe #22. Enclosed please find a motion to sever/dismiss and to quash the subpoena. Enclosed please find a money order in the amount of $46 representing the filing fee.

Date: 8/15/12

J Doe

John Doe #22, IP Address 69.126.229.98

Pro Se

Case 3:12-cv-03896-MAS-DEA Document 8 Filed 08/22/12 Page 16 of 16 PageID: 159

Clarkson S. Fisher Bldg & US Courthouse
402 East State St.
Trenton, NJ 08608

Re: Malibu Media, LLC v. Does1-30
Case No.: 3:12-cv-03896-JAP-DEA