

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA**

| | | |
|---------------------|---|---------------------------------|
| MALIBU MEDIA, LLC., |) | |
| |) | |
| Plaintiff, |) | Case No: 3:12-cv-00336-UAMH-JBT |
| |) | |
| v. |) | |
| |) | |
| JOHN DOES 1-18, |) | |
| |) | |
| Defendants. |) | |
| |) | |

PLAINTIFF’S MEMORANDUM IN OPPOSITION TO JOHN DOE 11’S MOTION TO SEVER & DISMISS AND FOR A PROTECTIVE ORDER [DKT. #16]

I. INTRODUCTION

Plaintiff respectfully requests the Court deny Defendant’s motion. Defendant creates a fictional picture of Plaintiff’s purpose in an effort to mislead and distract the Court from the serious copyright infringement claim brought by Plaintiff. As an initial point, Defendant’s Motion is based significantly on attacks to Plaintiff which are entirely unsubstantiated. “The only argument remaining—that copyright infringement suits of this sort are baseless ‘fishing expeditions’ used solely to extort money from alleged infringers—amounts to nothing more than an *ad hominem* attack on the Plaintiff. This line of argument fails to persuade.” AF Holdings, LLC v. Does 1-162, 11-23036-CIV, 2012 WL 488217 at *1 (S.D. Fla. Feb. 14, 2012). Plaintiff Malibu Media’s motivation for bringing these suits is quite simply to hold the infringers liable for their theft and by so doing hopefully deters the future theft of its movies. If there were an easier way to stop the infringement, Malibu Media would immediately pursue it.

Both the Eighth and Second Circuits, the only circuits to rule on this issue, have approved the use of Rule 45 subpoenas in on-line infringement cases to identify anonymous Doe Defendants. The Eight Circuit held “organizations such as the RIAA can file a John Doe suit,

along with a motion for third-party discovery of the identity of the otherwise anonymous ‘John Doe’ defendant.” In re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, FN3 (8th Cir. 2005). Similarly, in Arista Records, LLC. v. Doe 3, 604 F.3d 110 (2d Cir. 2010) the Second Circuit upheld the District Court’s denial of a motion to quash after Arista obtained leave “to serve a subpoena on defendants’ common ISP, the State University of New York at Albany.” By so holding, the Second Circuit approved the process of issuing a Rule 45 subpoena to an ISP to identify anonymous Doe Defendants. Doe 3 in the Arista case unsuccessfully argued he or she had a First Amendment right to remain anonymous that outweighed a Plaintiff’s right under the Petition Clause of the U.S. Constitution to sue for copyright infringement. Additionally, the Second Circuit rejected Doe 3’s assertion that the Supreme Court’s heightened pleading standards as announced in Bell Atlantic Corp. v. Twombly, 550 U.S. 544 (2007) and Ashcroft v. Iqbal, 129 S.Ct. 1337 (2009) made it impossible to plead a claim of infringement against an on-line anonymous infringer.

Just this week this Court issued a Report and Recommendation on this issue, stating “[t]he Court recognizes that each Defendant may later present different factual and substantive legal defenses, but that does not defeat, at this stage of the proceedings, the commonality in facts and legal claims that support joinder under Rule 20(a)(2)(B).” Malibu Media v. John Does 1-13, 2:12-cv-0177-JES-SPC (M.D. Fl. June 6, 2012) (Ex. A).

Both the Middle District of Florida and the Southern District of Florida have also issued opinions holding joinder is proper in copyright infringement BitTorrent actions at this stage of the litigation process and that plaintiffs have demonstrated good cause to receive discovery to identify the anonymous Doe Defendants. See Nu Image, Inc. v. Does 1-3,932, 2:11-CV-545-FTM-29, 2012 WL 646070 (M.D. Fla. Feb. 28, 2012) (“[t]he Court recommends that Defendant's improper joinder argument should fail”); see also AF Holdings, LLC v. Does 1-162,

11-23036-CIV, 2012 WL 488217, at *4 (S.D. Fla. Feb. 14, 2012) (“[a]s other courts have found, joinder of Doe Defendants is appropriate under such circumstances”).

Further, “the overwhelming majority of courts have denied as premature motions to sever prior to discovery.” First Time Videos, LLC v. Does 1-76, 2011 WL 3586245 (N.D. IL 2011) (citing a long list of cases holding joinder is proper). If, as Defendant urges, the Court were to sever all Doe defendants at this stage of the litigation process, Plaintiff would likely be unable to identify the remaining defendants due to the short time period that Internet Service Providers maintain their logs. Plaintiff would have to file 35 individual law suits and discovery requests, needlessly consuming the Court’s resources. If the ISPs delete their logs of user information during this time, Plaintiff will be unable to protect its copyright. Defendant is clearly aware of the difficulty Plaintiff would incur if this Court severed the present suit. Defendant does not actually want to be sued individually, but instead hopes that by severing the suit, Plaintiff will be delayed and suffer needless litigation costs while trying to obtain the identity of the Doe Defendants, who may not be identifiable by the time Plaintiff files each suit individually.

As explained below, the overwhelming majority of courts permit joinder in BitTorrent actions. Joinder is proper because the claims against all defendants are logically related and Plaintiff is seeking joint and several liability. Joinder in BitTorrent copyright infringement cases has been thoroughly analyzed in many opinions and has been permitted almost universally where, as here: (a) the complaint clearly explains how BitTorrent works through a series of transactions, (b) all of the defendants live in the district (eliminating long-arm issues and venue), (c) all of the defendants were part of the same exact swarm of peer infringers as evidenced by a unique cryptographic hash value, and (d) Plaintiff pled that the Defendants’ are contributorily liable for each others’ infringement. Recently, a court in New York examined the issue and held joinder is proper, concluding:

[I]t is difficult to see how the sharing and downloading activity alleged in the Complaint—a series of individuals connecting either directly with each other or as part of a chain or “swarm” of connectivity designed to illegally copy and share the exact same copyrighted file—could *not* constitute a ‘series of transactions or occurrences’ for purposes of Rule 20(a).

Digital Sin, Inc. v. Does 1-176, 2012 WL 263491 (S.D.N.Y. 2012); see also Patrick Collins, Inc. v. John Does 1-33, 2012 WL 415424 (D. Colo. 2012).

While courts have wide discretion to permit permissive joinder, this discretion must be exercised consistent with the requirement set forth in Rule 1 and the policy underlying Rule 20. Applying the existing law surrounding joinder to the facts in this case leads to but one inescapable conclusion: joinder is proper and should be permitted.

II. JOINDER IS PROPER

The Middle District of Florida has consistently found the actions of the Defendants in copyright infringement cases are sufficient to meet the standards of joinder. See K-Beech Inc., v. John Does 1-57, Case 2:11-cv-00358-CEH-SPC (M.D. Fl. 2011); see also Nu Image, Inc. v. Does 1-3,932, 2:11-CV-545-FTM-29, 2012 WL 646070 (M.D. Fla. Feb. 28, 2012).

Based on these allegations, the Court finds that Plaintiff's claims against the Defendants are logically related. Each John Doe Defendant is a possible source for the Plaintiff's work, and may be responsible for distributing the movie to other John Doe Defendants, who are also using the same file-sharing protocol to copy the identical copyrighted material.

Id.

A. The Infringement Occurred Through a Series of Transactions

For the word “series” to have any meaning in Rule 20(a), the rule must permit joinder to be proper when there is something other than a direct transaction. “Series” has been interpreted by Circuit Courts to mean a “logically related” fact pattern.

[A]ll ‘logically related’ events entitling a person to institute a legal action against another generally are regarded as comprising a transaction or occurrence. The analogous interpretation of the terms as used in Rule 20 would permit all reasonably related claims for relief by or against different parties to be tried in a

single proceeding. Absolute identity of all events is unnecessary.

Mosley v. Gen. Motors Corp., 497 F.2d 1330, 1333 (8th Cir. 1974).

While the logical relationship test does not require it, should this matter go to trial, Plaintiff will prove that the Defendants' infringement was committed through the same transaction or through a series of transactions with mathematical certainty by demonstrating, *inter alia*, that the algorithm used by BitTorrent Trackers would have caused the entire series of transactions to be different but for each of the Defendants' infringements.

i. Series of Transactions Explained By the Michigan Court

Recently, Judge Randon in the Eastern District of Michigan properly analyzed the facts in a near identical case, expanding substantial effort to understand the allegations in the complaint and the applicable law. Judge Randon summarized the plaintiff's allegation asserting that each Defendant copied the same piece of the same file as follows:

Plaintiff alleges that its investigator ("IPP") was able to download at least one piece of the copyrighted Movie from each Defendant (Dkt. No. 1 at 8–10). It is important to understand the implications of this allegation before determining whether joinder is proper. If IPP downloaded a piece of Plaintiff's copyrighted Movie from each Defendant (and, conversely, each Defendant uploaded at least one piece of the Movie to IPP) then each Defendant had at least one piece of the Movie—traceable via Hash Identifier to the same Initial Seeder—on his or her computer and allowed other peers to download pieces of the Movie.

By way of illustration: IPP's computer connected with a tracker, got the IP address of each of Defendants' computers, connected with each Defendants' computer, and downloaded at least one piece of the Movie from each Defendants' computer. During this transaction, IPP's computer verified that each Defendants' piece of the Movie had the expected Hash; otherwise, the download would not have occurred.

Patrick Collins, Inc. v. John Does 1-21, CIV.A. 11-15232, 2012 WL 1190840, at *4-5 (E.D. Mich. Apr. 5, 2012). Significantly, Judge Randon then explained through the force of clear deductive logic that each Defendant obtained the piece of plaintiff's movie in one of four ways all of which relate directly back to one individual seed.

If Plaintiffs allegations are true, each Defendant must have downloaded the piece(s) each had on his or her computer in one, or more, of the following four ways:

- 1) the Defendant connected to and transferred a piece of the Movie **from the initial seeder**; or
- 2) the Defendant connected to and transferred a piece of the Movie **from a seeder** who downloaded the completed file from the initial seeder or from other peers; or
- 3) the Defendant connected to and transferred a piece of the Movie **from other Defendants** who downloaded from the initial seeder or from other peers; or
- 4) the Defendant connected to and transferred a piece of the Movie **from other peers** who downloaded from other Defendants, other peers, other Seeders, or the Initial Seeder.

In other words, in the universe of possible transactions, at some point, each Defendant downloaded a piece of the Movie, which had been transferred through a series of uploads and downloads from the Initial Seeder, through other users or directly, to each Defendant, and finally to IPP.

Id. Having limited the universe to four possibilities the court correctly concluded the transaction was logically related.

Therefore, each Defendant is logically related to every other Defendant because they were all part of a series of transactions linked to a unique Initial Seeder and to each other. This relatedness arises not merely because of their common use of the BitTorrent protocol, but because each Defendant affirmatively chose to download the same Torrent file that was created by the same initial seeder, intending to: 1) utilize other users' computers to download pieces of the same Movie, and 2) allow his or her own computer to be used in the infringement by other peers and Defendants in the same swarm.

Id.

ii. It Is Not Necessary that the Defendants Shared the Infringing Movie With Each Other

Defendant's requirement of a direct defendant to defendant connection is a rigid approach to joinder, contrary to Supreme Court precedent. "Under the Rules, the impulse is toward entertaining the broadest possible scope of action consistent with fairness to the parties; joinder of claims, parties and remedies is strongly encouraged." United Mine Workers of Am. v. Gibbs, 383 U.S. 715, 724 (1966). "The touchstone of Rule 20 joinder/severance analysis is whether the interests of efficiency and judicial economy would be advanced by allowing the claims to travel

together, and whether any party would be prejudiced if they did.” Acciard v. Whitney, 2:07-CV-476UA-DNF, 2008 WL 5120820 (M.D. Fla. Dec. 4, 2008).

a. Defendant’s Test Was Directly Criticized By Courts

The Honorable Mary McLaughlin from the Eastern District of Pennsylvania, former Chief Counsel to the US Senate for the Subcommittee on Terrorism, Technology, and Government, recently addressed this exact issue in a similar BitTorrent copyright infringement action. Judge McLaughlin held joinder was proper even if the Doe defendants did not transmit the pieces directly to each other because the claims arise out of the same series of transactions. Raw Films v. John Does 1-15, 2012 WL 1019067, at *4 (E.D. Pa. March 26, 2012).

[E]ven if no Doe defendant directly transmitted a piece of the Work to another Doe defendant, the Court is satisfied at this stage of the litigation the claims against each Doe defendant appear to arise out of the same series of transactions or occurrences, namely, the transmission of pieces of the same copy of the Work to the same investigative server.

Id.

b. The Supreme Court Allows Joinder When There is No One to One Transaction

In United States v. Mississippi, 380 U.S. 128 (1965) the Supreme Court found that the joinder of six defendants, election registrars of six different counties, was proper because the allegations were all based on the same state-wide system designed to enforce the voter registration laws in a way that would deprive African Americans of the right to vote. Although the complaint did not allege that the registrars directly interacted with each other, or even that they knew of each other’s actions, or that each other’s actions directly affected each other in any way, the Supreme Court interpreted Rule 20 to hold a right to relief severally because the series of transactions were related and contained a common law and fact. Id. at 142-143.

[T]he complaint charged that the registrars had acted and were continuing to act as part of a state-wide system designed to enforce the registration laws in a way that would inevitably deprive colored people of the right to vote solely because of

their color. On such an allegation the joinder of all the registrars as defendants in a single suit is authorized by Rule 20(a) of the Federal Rules of Civil Procedure.

Id. at 142. Indeed, the Supreme Court held all of the defendants were joined properly because they were all acting on the basis of the same system which created a transactional relatedness.

Likewise, in the case at hand, it is not necessary for each of the defendants to have directly interacted with each other defendant, or have shared a piece of the file with each and every defendant when downloading the movie. The defendants are properly joined because their actions directly relate back to the same initial seed of the swarm, and their alleged infringement further advances the series of infringements that began with that initial seed and continued through other infringers. In doing so, the Defendants all acted under the same exact system. Just as it was not alleged in United States v. Mississippi that the registrars shared with each other their efforts to prevent African Americans from voting, it is not necessary for the defendants to have shared the pieces of the movie with each other. It is sufficient that the defendants shared pieces that originated from the same exact file, and opened their computer to allow others to connect and receive these pieces.

B. The Time Period For Infringement

The nature of the BitTorrent protocol provides for continuous seeding and distributing of the movie long after it has downloaded. Without stopping the program by physically unchecking the automatic seeding, an alleged infringer likely will seed and distribute a movie for an extended period of time. As the Eastern District of Michigan explained the technology, even after an infringer has completed a download of the movie, he or she may distribute the movie for weeks after having received the download.

[I]t is not that an infringer would wait six weeks to receive the Movie, it is that the infringer receives the Movie in a few hours and then leaves his or her computer on with the Client Program uploading the Movie to other peers for six weeks. Because the Client Program's default setting (unless disabled) is to begin

uploading a piece as soon as it is received and verified against the expected Hash, it is not difficult to believe that a Defendant who downloaded the Movie on day one, would have uploaded the Movie to another Defendant or peer six weeks later. This consideration, however, is irrelevant since concerted action is not required for joinder.

Patrick Collins, Inc. v. John Does 1-21, 2012 WL 1190840 (E.D. Mich. Apr. 5, 2012). Here, Plaintiff's investigator received a piece of the movie from the defendants when they were allegedly distributing it to others.

The Michigan Court further explained that time constraints should not impact that the infringements occurred through a series of transactions. "[T]he law of joinder does not have as a precondition that there be temporal distance or temporal overlap; it is enough that the alleged BitTorrent infringers participated in the same series of uploads and downloads in the same swarm." Patrick Collins, Inc. v. John Does 1-21, 2012 WL 1190840 (E.D. Mich. Apr. 5, 2012.)

a. The Time Period Amongst the Defendants is Reasonable Under Eleventh Circuit Case Law

In Alexander v. Fulton County, Ga., 207 F.3d 1303 (11th Cir. 2000) overruled on other grounds by Manders v. Lee, 338 F.3d 1304 (11th Cir. 2003) the Eleventh Circuit held a short time frame existed when the actions by the defendant took place within a year.

As for the first requirement, all of the Plaintiffs' claims stem from the same core allegation that they were subject to a systemic pattern or practice of race-based discrimination against white law enforcement officers by Sheriff Barrett in her first year in office. Plaintiffs all seek relief based on the same series of discriminatory transactions by the same decision-maker in the same department during the same short time frame.

Id. at 1324. (Emphasis added). Here, all of the defendants engaged in the same systematic pattern of infringement. And the time frame between the defendants on Exhibit A of the Complaint is only a total span of twelve weeks from the first hit date to the last hit date.

b. Other Courts Have Held the Time Frame in BitTorrent Actions is Irrelevant

The Northern District of California has also explained why the time gap in BitTorrent infringement cases does not impact the basic principles of joinder. “While this period might seem protracted, such time periods can be somewhat arbitrary in BitTorrent-based cases as long as the alleged defendants participate in the same swarm, downloading and uploading the same file.” First Time Videos, LLC v. Does 1-95, C 11-3822 MEJ, 2011 WL 4724882 (N.D. Cal. Oct. 7, 2011). “[E]ven after a Doe Defendant disconnects from the swarm, the parts of the file that he downloaded and uploaded will continue to be transferred to other Doe Defendants remaining in the swarm.” Id.

Other courts, when ruling on the issue of joinder have held that even when conduct occurs over a lengthy period of time, defendants may still be properly joined as long as the conduct is reasonably related. See Kedra v. City of Philadelphia, 454 F. Supp. 652, 662 (E.D. Pa. 1978) (holding joinder is proper when claims against police officers including unlawful searches, detentions, beatings and similar occurrences of multiple plaintiffs took place over a period of time).

There is no logical reason why the systematic conduct alleged could not extend over a lengthy time period and, on the face of these allegations, there is nothing about the extended time span that attenuates the factual relationship among all of these events. The claims against the defendants “aris(e) out of the same transaction, occurrence, or series of transactions or occurrences” for purposes of Rule 20(a), and therefore joinder of defendants in this case is proper.

Id. (Emphasis added). The case at hand is similar. While the actions of each of the defendants may have taken place over a period of time, the actions all arose from one initial seed and all display the same systematic conduct which is reasonably related.

C. Joinder is Proper Because Plaintiff Properly Pled Defendants Were Jointly and Severally Liable

The tests in the cases cited by Defendant requiring the defendants to directly send each other a piece of the movie further contradicts joinder principles because joinder is proper when a plaintiff pleads joint and several liability. See Genetic Technologies Ltd. v. Agilent Technologies, Inc., 11-CV-01389-WJM-KLM, 2012 WL 1060040 (D. Colo. Mar. 28, 2012) (“It is uncontested that Plaintiff does not assert joint or several liability here, which would be a separate basis for joinder.”)

Rule 20(a) provides for “any right to relief jointly, severally, or in the alternative”. In this case Plaintiff pled both joint and several liability.

Relief May be Sought “Jointly, Severally, or in the Alternative”: It is *not* necessary that each plaintiff or defendant be involved in every claim set forth in the complaint. Thus, for example, if there are several plaintiffs (e.g., driver and passenger in auto accident), each may seek *separate* relief. Likewise, if there are several defendants, relief may be sought against each of them separately, or against all of them jointly. [FRCP 20(a); *Dougherty v. Mieczkowski* (D DE 1987) 661 F.Supp. 267, 278]

Cal. Prac. Guide Fed. Civ. Pro. Before Trial Ch. 7-D. “[C]oncert of action, *i.e.*, a right to relief jointly, is not a precondition of joinder. Plaintiff asserts a right to relief jointly against Defendants *and* severally. Therefore, the first clause of Rule 20(a)(2)(A) is satisfied by the assertion of a right severally.” Patrick Collins, Inc. v. John Does 1-21, CIV.A. 11-15232, 2012 WL 1190840, at *8 (E.D. Mich. Apr. 5, 2012).

By requiring defendants to directly interact with each other, the Court would require the defendants to be jointly liable with each other. Because Rule 20 provides that a party may be joined if the claims against them are either jointly or severally liable, the requirement that defendants directly shared pieces of the movie with each other contradicts the language of Rule 20.

A right to relief against defendants jointly requires concerted action by two or more parties. A right to relief severally against defendants means that each right to relief is separate and distinct from defendant to defendant and no interaction

among the defendants is required. An ‘alternative’ right to relief may be asserted when plaintiff knows one of the defendants is liable, but does not know which one. 4 Moore's Federal Practice § 20.03. Plaintiff asserts a right to relief against Defendants jointly and a right to relief severally; however, a right to relief against the Defendants severally alone is sufficient to satisfy the first clause of Rule 20.

Id. (Emphasis added).

D. There Are Common Issues of Fact and Law

Rule 20(a)(2)(B) requires the plaintiffs' claims against the putative defendants to contain a common question of law or fact. “The Plaintiff meets this requirement. In each case, the Plaintiff will have to establish against each putative defendant the same legal claims concerning the validity of the copyrights in the movies at issue and the infringement of the exclusive rights reserved to the plaintiffs as copyright holders.” Nu Image, Inc. v. Does 1-3, 932, 2:11-CV-545-FTM-29, 2012 WL 1255189 (M.D. Fla. Apr. 12, 2012). The “factual issues related to how BitTorrent works and the methods used by plaintiffs to investigate, uncover and collect evidence about the infringing activity will be essentially identical for each putative defendant.” Call of the Wild Movie v. Does 1-1,062, 770 F. Supp. 2d 332, 344-345 (D.D.C. 2011).

E. Joinder Promotes Judicial Efficiency and is Beneficial to Putative Defendant and Doe Defendants Cannot Demonstrate Prejudice At This Stage

Joinder of the defendants creates judicial efficiency, particularly at this stage of the litigation process and is beneficial to the Doe Defendants. “The Court finds that joinder, at this stage of the litigation, will not prejudice any party and will promote judicial efficiency.” Patrick Collins, Inc. v. John Does 1-33, 11-CV-02163-CMA-MJW, 2012 WL 415424 (D. Colo. Feb. 8, 2012).

The Southern District of New York addressed this issue stating, “courts have opined that requiring aggrieved parties to file hundreds or even thousands of separate copyright infringement actions would neither be cost efficient for the plaintiffs nor promote convenience or judicial

economy for the courts.” Digital Sin, at FN 6.

Defendant unconvincingly argues that the Court should sever because the formal discovery process will be unmanageable for the Court and prejudice defendants. As an initial point, a joined case in the discovery process would likely benefit the defendants who would be able to see multiple discovery requests from different counsel. More importantly, if the Court at that time chooses to sever, it may. The Court may use its discretionary powers to sever at any time. But that does not change the fact that at this stage in the litigation process joinder is proper and in the interest of judicial efficiency.

III. THIS COURT SHOULD NOT ISSUE A PROTECTIVE ORDER

“The party ‘seeking a protective order carries the burden of showing good cause and/or the right to be protected.’” Nathai v. Florida Detroit Diesel-Allison, Inc., 3:09-CV-1-J-20HTS, 2009 WL 2424570 (M.D. Fla. Aug. 5, 2009). “To make a showing of good cause, the movant has the burden of showing the injury ‘with specificity.’” Trinos v. Quality Staffing Services Corp., 250 F.R.D. 696, 698 (S.D. Fla. 2008) (internal citations omitted).

The Southern District of Florida has twice denied similar defendants’ requests for Protective Orders. See Boy Racer, Inc. v. John Does 1-34, 11-23035, 2012 WL 1535703, at *3 (S.D. Fla. May 1, 2012) (following AF Holdings, LLC v. Does 1-162, 11-23036-CIV, 2012 WL 488217 (S.D. Fla. Feb. 14, 2012)).

The *AF Holdings* court also rejected the same type of extortion arguments raised in this case. In doing so, that court relied on the *Liberty Media Holdings* case for the notion that “the potential embarrassment or social stigma that [the Doe Defendants] may face once their identities are released in connection with this lawsuit is not grounds for allowing them to proceed anonymously.”

Id. at *4 (citing Liberty Media Holdings, LLC v. Swarm Sharing Hash File

AE340D0560129AFEE8D78CE07F2394C7B5BC9C05, 821 F. Supp. 2d 444 (D. Mass. 2011)).

A. The Information Plaintiff Requests is Relevant

This Court granted Plaintiff limited discovery to serve a subpoena on Defendant's ISP because Plaintiff has no other way to identify the Defendants and proceed with its copyright infringement case against them. Plaintiff has requested only the identifying information of the Defendants from their ISPs. As other courts have explained, the information Plaintiff seeks is highly relevant.

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).

The Eastern District of Pennsylvania 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 an unpublished opinion from the Northern District of Illinois to support his theory that Plaintiff's subpoena should be quashed. *See* Def's Mot. citing VPR Internationale v. Does 1-1017, 2:11-cv-02068, (C. Ill. March 8, 2011). VPR Internationale involved 1,017 defendants grouped into one case, and lacked personal jurisdiction and venue. This case does not suffer from the same procedural problems.

Defendant also relies heavily on the Eastern District of New York opinion where Judge

Brown questioned the likelihood the infringer was the owner of the IP Address. See Def's Mot. at ¶ 6. 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."¹ 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."² This article, published on March 26, 2012, runs contrary to Judge Brown's assertions and supports the idea that most households do have closed, protected wireless that are not likely to be used by a neighbor or interloper.

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.³

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

¹ See Free Wi-Fi is Gone Forever www.pcmag.com/article2/0,2817,2402137,00.asp (Attached as Ex. B).

² Id.

³ Statement of Deputy Assistant Attorney General Jason Weinstein Before the Senate Judiciary Subcommittee on Privacy, Technology and the Law available at www.justice.gov.

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.

B. The Doe Defendant’s IP Addresses Were Undoubtedly Used to Distribute Plaintiff’s Copyrighted Movie

Defendant references a study that concludes the best approach to accurately identify IP addresses is to establish a direct connection with the infringing user and verify the contents received:

A more thorough approach to detecting infringement in BitTorrent would be to adopt the stated industry practice for monitoring the Gnutella network: in the case of suspected infringement, download data directly from the suspected user and verify its contents. Because we have notified several enforcement agencies ... we expect increasing use of direct downloads for verifying information.⁴

(Emphasis added.) Plaintiff used this exact process to identify Defendant’s IP address. Plaintiff’s investigative service, IPP Limited, established a direct one to one connection with a computer using Defendant’s internet service and received a piece of Plaintiff’s copyrighted movie from that computer. “A direct and continuous connection between the IPTRACKER-server and the uploader of the file is established and exists at least 10 seconds before, during and at least 10 seconds after the capture sequence i.e. during the whole download process.” (Dec.

⁴ Def.’s Mot. 16 citing Michael Piatek, Tadayoshi Kohno, & Arvind Krishnamurthy, *Challenges and Directions for Monitoring P2P File Sharing Networks – or – Why My Printer Received a DMCA Takedown Notice*, 3rd USENIX Workshop on Hot Topics in Security (HatSec ’08), July 2008.

Tobias Feiser Ex. A. at *4.)

Further, as Defendant's study suggests, Plaintiff has taken additional safeguards for accuracy by verifying the content received from Defendant.⁵ Plaintiff has a human "in the loop" to provide a manual check of the identifying material. As Plaintiff's investigator, Tobias Fieser, attests, "I analysed each BitTorrent 'piece' distributed by each IP address listed on Exhibit B and verified that reassembling the pieces using a specialized BitTorrent Client results in a fully playable digital motion picture." (Dec. Tobias Fieser at ¶ 21.) Plaintiff is absolutely certain that Defendant's IP address downloaded, controlled, and distributed Plaintiff's copyrighted work to its investigative service. Defendant's study supports Plaintiff's findings.

C. Plaintiff Has A Proper Purpose

The online theft of Plaintiff's property greatly damages its business, products, and reputation. Accordingly, Plaintiff Malibu Media's motivation for bringing these suits is quite simply to hold the infringers liable for their theft and by so doing hopefully deter the future theft of its movies. If there was any easier way to stop the infringement, Malibu Media would immediately pursue it.

Both the Eighth and Second Circuits, the only circuits to rule on this issue, have approved the use of Rule 45 subpoenas in on-line infringement cases to identify anonymous Doe Defendants. The Eight Circuit held "organizations such as the RIAA can file a John Doe suit, along with a motion for third-party discovery of the identity of the otherwise anonymous 'John Doe' defendant." In re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, FN3 (8th Cir. 2005). Similarly, in Arista Records, LLC. v. Doe 3, 604 F.3d 110 (2d Cir. 2010) the Second Circuit upheld the District Court's denial of a motion to quash after Arista obtained leave "to serve a subpoena on defendants' common ISP, the State University of New

⁵ Piatek at *6.

York at Albany.” By so holding, the Second Circuit approved the process of issuing a Rule 45 subpoena to an ISP to identify anonymous Doe Defendants. Doe 3 in the Arista case unsuccessfully argued he or she had a First Amendment right to remain anonymous which outweighed a Plaintiff’s right under the Petition Clause of the U.S. Constitution to sue for copyright infringement. Additionally, the Second Circuit rejected Doe 3’s assertion that the Supreme Court’s heightened pleading standards as announced in Bell Atlantic Corp. v. Twombly, 550 U.S. 544 (2007) and Ashcroft v. Iqbal, 129 S.Ct. 1337 (2009) made it impossible to plead a claim of infringement against an on-line anonymous infringer.

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 identity. 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. Any such holding would be contrary to existing law and the express policy of Congress. In 1999 Congress intentionally amended the Copyright Act to deter individuals from infringing copyrights on the internet by increasing the statutory remedies:

Congress did contemplate that suits like this [against individuals] were within the Act. Congress last amended the Copyright Act in 1999 to increase the minimum and maximum awards available under § 504(c). See Digital Theft Deterrence and Copyright Damages Improvement Act of 1999, Pub. L. No. 106-160, 113 Stat. 1774. At the time, Congress specifically acknowledged that consumer-based, noncommercial use of copyrighted materials constituted actionable copyright infringement. Congress found that "copyright piracy of intellectual property flourishes, assisted in large part by today's world of advanced technologies," and cautioned that “the potential for this problem to worsen is great.”

Sony v. Tennenbaum, 2011 WL 4133920 at *11 (1st Cir. 2011) (emphasis added).

During her time as Register of Copyright, Mary Beth Peters explained the rights of copyright holders in peer-to-peer infringement actions to the Senate Judiciary Committee. “The law is unambiguous. Using peer-to-peer networks to copy or distribute copyrighted works

without permission is infringement and copyright owners have every right to invoke the power of the courts to combat such activity. Every court that has addressed the issue has agreed that this activity is infringement.”⁶ Ms. Peters further explained the significant need for exactly the type of copyright infringement claims that are before this Court:

[F]or some users of peer-to-peer technology, even knowledge that what they are doing is illegal will not be a sufficient disincentive to engage in such conduct. But whether or not these infringers know or care that it is against the law, the knowledge that such conduct may lead to expensive and burdensome litigation and a potentially large judgment should have a healthy deterrent effect. 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. For many people, the best form of education about copyright in the internet world is the threat of litigation. In short, if you break the law, you should be prepared to accept the consequences. Copyright owners have every right to enforce their rights in court, whether they are taking action against providers of peer-to-peer services designed to profit from copyright infringement or against the persons engaging in individual acts of infringement using such services.

Id. (Emphasis added).

D. Plaintiff's Settlements are Proper

Defendant mischaracterizes Plaintiff's purpose for engaging in settlement activities, suggesting that simply the fact that a Defendant named in litigation may be offered a settlement is an attempt at coercion and improper embarrassment. Prior to actually proceeding against defendants, it is proper to contact them to discuss settlement options. The only difference between this case and the countless others filed every day by other plaintiffs in a broad array of civil litigation is that the Plaintiff does not have the ability to identify the defendants before the suit is filed.

The Supreme Court has stated that public policy favors resolutions through settlement.

⁶ 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>

“Rule 68’s policy of encouraging settlements is neutral, favoring neither plaintiffs nor defendants; it expresses a clear policy of favoring settlement of all lawsuits.” Marek v. Chesny 473 U.S. 1, 11 (1985). Further, Plaintiff has a First Amendment right under the petition clause to make the demand. See Sosa v. DirectTV, 437 F. 3d 923, 937 (9th Cir. 2006) (holding “the protections of the Petition Clause extend to settlement demands as a class,” including those made during and prior to a suit.)

Just last week the Eastern District of Michigan addressed this issue, noting that a Defendant had provided no specific facts to support its claim that Plaintiff’s purpose was to scare up settlements. See Third Degree Films v. Does 1-36, 11-CV-15200 (E.D. Mich. May 29, 2012).

To the extent that it is independent, the Court notes that while Defendant claims that this suit was brought only to scare up settlements (Def.’s Mot. to Sever at 2, 11), Defendant has offered no case-specific facts supporting this claim. Rather, Defendant relies on the conduct of adult-film companies in other cases. This guilt-by-association argument does not justify quashing the subpoena that this Plaintiff, Third Degree Films, served on Defendant’s ISP pursuant to an Order entered by Judge Murphy allowing this discovery.

Id. (Emphasis added). Just as in Third Degree, Defendant is attempting to influence this Court to make a decision based on accusations in other cases involving other counsel and other plaintiffs. Indeed, Defendant cites to cases that can only refer to vague, anecdotal accusations of improper settlement tactics. These erroneous conclusions are propagated by anti-copyright blogs as a suggested defense strategy. The only example Defendant can offer of a so called “improper settlement tactic” is a situation where a plaintiff in an unrelated case, refused to engage in expensive, time consuming, and burdensome discovery of a putative doe defendant’s computer, before receiving the doe defendant’s information from its ISP and verifying the doe defendant was a proper party. See Def’s Mot. 17 (citing In re: BitTorrent Adult Film Copyright Infringement Cases, 2012 WL 1570765, at *5). It flies in the face of reason that this scenario would rise to the level of an improper settlement tactic.

While Defendant goes to substantial effort to decry Plaintiff's purpose and settlement attempts, Defendant cannot provide one specific example of improperly holding a defendant to account. These arguments are further unconvincing when Defendant is represented by counsel who should adequately be capable of preventing Defendant from any alleged hypothetical coercion.

III. CONCLUSION

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

Dated: June 12, 2012

Respectfully submitted,

By: /s/ M. Keith Lipscomb
M. Keith Lipscomb (429554)
klipsomb@lebfirm.com
LIPSCOMB EISENBERG & BAKER, PL
2 South Biscayne Blvd.
Penthouse 3800
Miami, FL 33131
Telephone: (786) 431-2228
Facsimile: (786) 431-2229
Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on June 12, 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/ M. Keith Lipscomb