TABLE OF CONTENTS

INTRODUCTION.....1

RELEVANT FACTUAL BACKGROUND….....1

ARGUMENT WITH RESPECT TO THE MOTION TO QUASH 6

I. DEFENDANT, JOHN DOE #25, HAS STANDING TO CONTEST THE SUBPOENA 6

II. THE SUBPOENA SHOULD BE QUASHED BECAUSE THE REQUESTED DISCOVERY INFORMATION DOES NOT ADVANCE PLAINTIFF'S CASE AND WOULD IMPOSE ANNOYANCE, EMBARASSMENT, AND UNDUE BURDEN.....7

ARGUMENT WITH RESPECT TO THE MOTION TO SEVER……...11

I. INTRODUCTION.....11

II. PLAINTIFF CANNOT MEET RULE 20'S TRANSACTIONAL COMPONENT…….13

III. JOINDER IS DISCRETIONARY WITH THE COURT TO ENSURE JUSTICE……..14

IV. PLAINTIFF MANIPULATES JOINDER TO AVOID PAYING FILING FEES…….15

CONCLUSION 16

TABLE OF AUTHORITIES

Federal Cases

Third Degree Films, Inc. v. Does 1-108, 2012 U.S. Dist. LEXIS 25400 (D.Md. Feb. 28, 2012).....6

Wiwa v. Royal Dutch Petroleum Co., 392 F.3d 812, 820 (5th Cir. 2004).....7

Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 580 (N.D.Cal. 1999)…… ……..……..8

In re BitTorrent Adult Film Copyright Infringement Cases, 2012 U.S. Dist. LEXIS 61447 [*8] (E.D.N.Y. May 1, 2012)…….8, 13

VPR Internationale v. Does 1-1017, 2011 U.S. Dist. LEXIS 64656 (C.D.Ill. Apr. 29, 2011)…….…… ……..….9, 10

Raw Films, Ltd. v. Does 1-32, 2011 U.S. Dist. LEXIS 149215, 2011 WL 6840590, at *2 (N.D.Ga. Dec. 29, 2011)……... 14

Raw Films, Ltd. v. Does 1-32, 2011 U.S. Dist. LEXIS 114996, 2011 WL 6182025, at *2 (E.D.Va. 2011)……...……...……14

Pac. Century Int'l Ltd. v. Does 1-101, 2011 U.S. Dist. LEXIS 124518 (N.D.Cal. Oct. 27, 2011)……. ……..15

In re Diet Drugs, 325 F. Supp. 2d 540, 541-42 (E.D.Pa. 2004) ……...15

Pac. Century Int'l Ltd. v. Does 1-37, 2012 U.S. Dist. LEXIS 44368 [*3] (N.D.Ill. Mar. 30, 2012)……..….5, 16

Federal Rules

Fed. R. Civ. P. 45(c)(3)(A)(iv).....7

Fed. R. Civ. P. 26.....7

Fed. R. Civ. P. 26(b)(1).....7

Fed. R. Civ. P. 26(c)…….....7, 8

Fed. R. Civ. P. 20(a)(2).....12

Fed. R. Civ. P. 20(b).....12

Fed. R. Civ. P. 21.....12, 14

Fed. R. Civ. P. 1.....14

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

MALIBU MEDIA, LLC,	:	
	:	Civil Action No. 3:12-cv-03896-JAP-DEA
Plaintiff,	:	
	:	
v.	:	
	:	
JOHN DOES # 1-30,	:	
	:	
Defendants.	:	

BRIEF IN SUPPORT OF: MOTION TO QUASH PLAINTIFF'S RULE 45 SUBPOENA AND MOTION TO SEVER PLAINTIFF PURSUANT TO RULE 21
BY DEFENDANT JOHN DOE #25

John Doe #25 (named as having IP address 108.35.214.163) ("Defendant"), by and through counselor Michael Mignogna for the firm Mattleman, Weinroth & Miller, P.C., hereby moves to quash the subpoena or, in the alternative, moves to have the Court sever him from the other John Doe Defendants in the instant case. Defendant cites the following in support:

I. FACTUAL BACKGROUND

Malibu Media, LLC, ("Plaintiff") is a company domiciled in the State of California. Plaintiff alleges that he created the copyright items at issue in the instant litigation, pornographic films whose names are too unsavory to be repeated.

Defendant John Doe #25 is an individual who wishes to remain anonymous. Defendant's Internet Service Provider ("ISP") is Verizon. According to Verizon's

records from the time of the alleged incident, Defendant's IP ("Internet Protocol") address was 108.35.214.163. That IP address, along with numerous others, has been named as involved in the swarm of file-sharing which forms the basis for this lawsuit.

Plaintiff alleges that John Does #1-30 infringed upon the copyright to the films. Plaintiff alleges the Does participated in a file-sharing "swarm" using BitTorrent over the course of the months of March, April and May 2012. (Plaintiff's Exhibit A). A "swarm," sometimes called a multisource or segmented downloading method, is a means by which users of BitTorrent can simultaneously download and share the same file without need of a single host.

The BitTorrent protocol allows users to transfer files over the Internet. Like virtually any file-sharing technology, BitTorrent may be used to legally upload or download computer files. It may also be used to pirate copyrighted software, music, movies, and other computer-accessible media. Unlike other file-sharing technology, in which users connect to one another or to a central repository to transfer files, files shared via BitTorrent exist in a swarm, with pieces of the whole file distributed among the users. The following example illustrates this technology in action: (1) the original user posts a 100 MB movie file on a BitTorrent tracker website. The file exists only on that original user's computer—the file is not uploaded to the tracker website, (2) other users discover this movie file through the

tracker website and log onto the BitTorrent swarm to download the file, (3) on the original user's computer, BitTorrent software divides the 100 MB movie into 10,000 pieces, each representing a 10 kB "packet" or piece, (4) as other downloaders log onto the BitTorrent swarm, these 10 kB pieces are randomly distributed—the first piece to the first downloader, the second piece to the second downloader, etc., (5) after the initial packets are transferred, additional packets are randomly transferred to the downloaders so that the first downloader may have the first and 500th piece, the second the second and 900th to the second, etc., (6) once enough packets have been distributed to downloaders in the swarm, the BitTorrent protocol will automatically transfer pieces between downloaders so that the first downloader may receive the 900th piece from the second downloader and the second downloader may receive the first piece from the first downloader, etc., (7) the BitTorrent swarm becomes larger as more people—from around the world—log in and more pieces are distributed, (8) once every piece of the original file has been uploaded to the collective swarm, the original downloader may log off—the entire movie exists in packets among the swarm, (9) when a downloader has received all 10,000 kB packets of the 100 MB file, his BitTorrent software restructures the data so as to reconstruct a copy of the original file on his computer, finally (10) these completed downloaders may now log off, or they may remain online to continue seeding pieces of the file to other downloaders.

There are several nuances about the BitTorrent protocol. First, every participant may upload and download pieces of the file essentially simultaneously. Second, these individual pieces are useless until a user has all of them. The user cannot reassemble the original file with even 99% of the pieces. Third, a user may log on and download just one piece (e.g. a 10 kB piece) of the file and log off, waiting to download other pieces later or discarding the downloaded pieces entirely. Fourth, a BitTorrent user may restrict his software settings so as to only permit downloads and not uploads.

Plaintiff's suit is but one among a blizzard of mass copyright infringement suits that have recently swept through state and federal courts around the nation. These copyright infringement lawsuits have largely focused on the BitTorrent family of protocols. On July 3, 2012, Plaintiff was granted leave to take expedited discovery pursuant to a Rule 26(f) conference and issuance of a Rule 45 subpoena. The Plaintiff will then seek to link the IP addresses to the names and mailing addresses of Internet subscribers.

Upon information and belief, Defendant asserts that none of these cases have been brought to trial. In the rare instance in which a John Doe raises a defense or counter-claims, the plaintiffs abandon any attempt to pursue their case. Instead, the plaintiffs' strategy has been (a) to collect personal identifying information concerning the various John Doe defendants via early discovery, and then (b) to

send a threatening letter to each defendant alleging copyright infringement while demanding a settlement payment to dismiss the claims. The settlement payments are usually in the thousands of dollars per defendant. Chief among the coercive elements of the plaintiffs' strategy is the insinuation of public disclosure. The plaintiffs warn, barring receipt of a substantial settlement amount, that the defendant's name will appear alongside the allegations of copyright infringement of a film, the title of which is usually obnoxious and vulgar. *See, e.g., Pac. Century Int'l, Ltd. v. Does 1-37*, 2012 U.S. Dist. LEXIS 44368 (N.D. Ill. Mar. 30, 2012).

Plaintiff lacks the desire to prove his case on the merits; rather, he engages in a fishing expedition to hassle, embarrass (given the pornographic character of the film) and extract payment from Doe Defendants. As noted above, individual file packets are useless. Without the remaining pieces, a single Doe Defendant cannot do anything with this scrap of data. If it is the case that each Doe Defendant actually logged into a BitTorrent swarm, a questionable premise as explained *infra*, downloaded without the complete file and then logged off, all he has done is receive an unusable fragment of a copyrighted work.

An IP address issued to an Internet subscriber is not necessarily linked to just one computer. In fact, by means of a fairly common, inexpensive wireless router, an Internet subscriber's IP address can be accessed by numerous people. Without the Internet subscriber's knowledge or consent, someone else may have

joined into a file-sharing swarm. This may be true even if the Internet subscriber had attempted to secure his wireless connection with a password. Given the inevitability of wireless Internet sharing and insecurity, the plaintiffs in these types of lawsuits may well have only the slightest speculation that any of the named defendants actually infringed on the plaintiffs' copyright. Worse, the plaintiffs conceal their true objective—scaring the defendants into paying thousands of dollars in settlement—within litigation documents riddled with attenuated legal theories joinder, discovery, and more.

II. ARGUMENT WITH RESPECT TO THE MOTION TO QUASH

1. DEFENDANT, JOHN DOE #25, HAS STANDING TO CONTEST THE SUBPOENA

The threshold issue in a Motion to Quash is that of standing. Plaintiff seeks disclosure of Defendant's confidential, personal identity information. This information is shared only between the Defendant, as an Internet subscriber, and his ISP. Indeed, as the nature of Plaintiff's Complaint itself demonstrates, a subscriber's IP address is anonymous except for the fact that it discloses his general location and ISP. Consequently, the Defendant has privacy and proprietary interests over the information sought after in this subpoena; he may, therefore, move to quash the subpoena. *See, e.g., Third Degree Films, Inc. v. Does 1-108,*

2012 U.S. Dist. LEXIS 25400 (D. Md. Feb. 28, 2012). In the alternative, Defendant has standing to move to quash the subpoena to prevent an undue burden under Fed. R. Civ. P. 45(c)(3)(A)(iv) or because the subpoena would subject him to annoyance or embarrassment as outlined in Fed. R. Civ. P. 26.

2. THE SUBPOENA SHOULD BE QUASHED BECAUSE THE REQUESTED DISCOVERY INFORMATION DOES NOT ADVANCE PLAINTIFF'S CASE AND WOULD IMPOSE ANNOYANCE, EMBARASSEMENT, AND AN UNDUE BURDEN

Plaintiff, through his subpoena, seeks information that is neither relevant to pursuing his claim nor which takes effort to relieve the Doe Defendants of unnecessary annoyance or embarrassment. Generally, the scope of discovery is broad and permits the discovery of "any nonprivileged matter that is relevant to any party's claim or defense." Fed. R. Civ. P. 26(b)(1). A discovery request is relevant when the request seeks admissible evidence or "is reasonably calculated to lead to the discovery of admissible evidence." *Wiwa v. Royal Dutch Petroleum Co.*, 392 F.3d 812, 820 (5th Cir. 2004) (citation and internal marks omitted). Federal Rule 45(c)(3)(A)(iv) authorizes the court to quash a subpoena to protect a person from "undue burden." Additionally, Rule 26(c) permits a court to make

"any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Fed. R. Civ. P. 26(c).

In order to be eligible for early discovery, Plaintiff must demonstrate a reasonable likelihood that the requested discovery will lead to identification of the Doe Defendant. *See Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 580 (N.D. Cal. 1999). But, given the nature of file-sharing technology, an IP address is not necessarily correlated with the individual targeted in an allegation of copyright infringement. This is because an IP address is issued to an Internet *subscriber*—not to any particular computer or individual. In fact, the District Court for the Eastern District of New York recently stated: "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." *In re BitTorrent Adult Film Copyright Infringement Cases*, 2012 U.S. Dist. LEXIS 61447 [*8] (E.D.N.Y. May 1, 2012).

Briefly, when an ISP issues an Internet subscription, the subscriber is issued an IP address. The subscriber can use a wireless router to transmit Internet access, using the same IP address, to any computer within several hundred feet of the router. With modern, powerful wireless routers, the connection distance can be quite large. Wireless routers are becoming increasingly common throughout the nation. Some estimate that wireless routers are used by nearly 61% of all U.S.

homes. Lardinois, F,. "Study: 61% of US Households Now Have WiFi," available at http://techcrunch.com, 4/5/12.

Plaintiff makes the bald assertion in his Complaint that each Defendant (Internet subscriber) was also a peer member to a swarm. (Plaintiff's Complaint, paragraph 33). What Plaintiff neglects to add is that the subscribers to whom IP addresses were issued, even if their wireless routers were password secured, may not actually be the same person who allegedly shared the file at issue in the instant litigation. In similar litigation, the District Court for the Central District of Illinois pointed out that:

> IP subscribers are not necessarily copyright infringers. Carolyn Thompson writes in an MSNBC article of a raid by federal agents on a home that was linked to downloaded child pornography. The identity and location of the subscriber were provided by the ISP. The desktop computer, iPhones, and iPads of the homeowner and his wife were seized in the raid. Federal agents returned the equipment after determining that no one at the home had downloaded the illegal material. Agents eventually traced the downloads to a neighbor who had used multiple IP subscribers' Wi-Fi connections (including a secure connection from the State University of New York).

VPR Internationale v. Does 1-1017, 2011 U.S. Dist. LEXIS 64656 (C.D. Ill. Apr. 29, 2011) (citing Thompson, C., "Bizarre Pornography Raid Underscores Wi-Fi Privacy Risks," available at http://www.msnbc.msn.com/id/42740201/ns/technology_and_science-wireless, 4/25/11.

The Court then went on to explain that "[w]here an IP address might actually identify an individual subscriber . . . the infringer might be the subscriber, someone in the subscriber's household, a visitor with her laptop, a neighbor, *or someone*

parked on the street at any given moment." *VPR Internationale v. Does 1-1017*, 2011 U.S. Dist. LEXIS 64656 (C.D. Ill. Apr. 29, 2011) (emphasis supplied).

An additional problem is presented by IP spoofing. The most basic tool by which information is transferred online is the IP. An IP contains a numerical source and destination code, from which an "IP address" can be gleaned. The source address is normally from which an information packet was sent. By forging headers in information packets, however, an Internet user can conceal his true location behind the forged IP address of another. This forging process is relatively simple and is commonly referred to as "spoofing." In the instant litigation, the actual copyright infringer could have mimicked the IP address of a named John Doe. The legitimate holder of an IP address, meanwhile, would have no way of knowing that somebody else was masquerading online with his IP address. Plaintiff presents no proof that his named IP addresses are legitimate and not the product of spoofing technology. Plaintiff seems to have recklessly run the risk that its named IP addresses are not even the correct IP addresses from which he as attempting to collect identifying information.

Defendant John Doe #25 incorporates an Affidavit to this Brief clarifying that his suburban home has a wireless ("WiFi") Internet router (Affidavit of John Doe #25). Doe #25 also attests that, to his knowledge, neither he nor anybody in his household knew who else could have been in the swarm. His computer was, in

fact, set to a schedule that would have kept it off during the date and time in question. Neighbors and their social guests, however, could have been within range of his WiFi signal. In other words, the correct party to be sued in this lawsuit is neither named nor likely ever to be found.

Perhaps unsurprisingly, Plaintiff does not explain in any detail how he has gathered the IP addresses of these John Doe Defendants. Instead, we are told he hired a company headquartered out of Thailand, IPP Limited, to use a commonly-sold commercial software product, International IPTracker, to scan “peer-to-peer networks for the presence of infringing transactions.” Specifically, no mention is made of (a) the education and expertise, if any, of the persons assembling this information, or (b) how accurate this company’s practices have been in actually identifying the correct defendants in the past.

III. ARGUMENT WITH RESPECT TO THE MOTION TO SEVER

1. INTRODUCTION

The Federal Rules set forth the requirements for permissive joinder: "Persons . . . may be joined in one action as defendants if: (A) any right to relief [is] asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction or occurrence or series of transactions or occurrences; and (B) any question of law or fact common to all defendants will

arise in the action." Fed R. Civ. P. 20(a)(2). The Federal Rules also provide that "[t]he court may issue orders—including an order for separate trials—to protect a party against embarrassment, delay, expense, or other prejudice that arises from including a person against whom the party asserts no claim and who asserts no claim against the party." Fed R. Civ. P. 20(b). Additionally, the Court, on its own or by motion, may drop a party as provided by Federal Rule 21.

Plaintiff's contention is that individuals joining anonymously into a swarm, enduring over the course of two months, were somehow coordinated in their activity. He then argues that each individual was involved in the same "transaction," "occurrence," or "series of transactions or occurrences." Plaintiff makes the utterly baseless assertion that Defendants were "acting in concert with each other" (Plaintiff's Complaint, paragraph 10). In the instant situation, the connection into the swarm at issue would have taken place without the knowledge or consent of the Internet subscriber actually targeted in the lawsuit.

When a BitTorrent user begins using the software, he has no idea who the other members of the swarm may be. They may be from Swedesboro, New Jersey or they may be from Sweden. The only information available to the BitTorrent user is how many other users are connected into the swarm. Because there may be potentially thousands of individuals in the swarm, it is possible none of the named

Doe Defendants in this action ever participated in the swarm at the same with one another—even inadvertently.

2. PLAINTIFF CANNOT MEET RULE 20'S TRANSACTIONAL COMPONENT

District Courts in similar matters have found misjoinder, usually on the deficiency in Rule 20's transactional component—holding that the Doe Defendants' separate and distinct circumstances would not constitute the same "transaction," "occurrence," or "series of transactions or occurrences." In perhaps the best explanation of why joinder is inappropriate in these cases, a judge in the District Court for the Eastern District of New York noted that, as a practical matter, it is unclear whether a Doe Defendant could have "act[ed] in concert" with others as part of some act to infringe on the plaintiff's copyright." *In re BitTorrent Adult Film Copyright Infringement Cases,* 2012 U.S. Dist. LEXIS 61447 (E.D.N.Y. May 1, 2012). As the Court remarked, "[m]uch of the BitTorrent protocol operates invisibly to the user—after downloading a file, subsequent uploading takes place automatically if the user fails to close the program." *Id.* In addition, the Court noted that it seemed less plausible to accept the notion that the Doe Defendants acted in concert with one another because the dates of alleged downloading in the complaints were sometimes weeks or months apart. *Id.*

Courts in other Districts have refused to find joinder proper when a single swarm was at issue. *See generally Raw Films, Ltd. v. Does 1-32*, 2011 U.S. Dist. LEXIS 149215, 2011 WL 6840590, at *2 (N.D.Ga. Dec. 29, 2011) (stating that the "differing dates and times of each Defendant's alleged sharing do not allow for an inference that the Defendants were acting in concert"); *Raw Films, Ltd. v. Does 1-32*, 2011 U.S. Dist. LEXIS 114996, 2011 WL 6182025 at *2 (E.D.Va. 2011) (conduct over a three month time span was "insufficient to meet the standards of joinder set forth in Rule 20").

3. JOINDER IS DISCRETIONARY WITH THE COURT TO ENSURE JUSTICE

Additionally, because joinder is discretionary with the Court, the Court would retain the ability to sever a defendant to comport with principles of justice and fairness. Fed R. Civ. P. 21. Federal Rule of Civil Procedure 1 advises that the Rules should be construed to provide “just, speedy, and inexpensive determination” of civil disputes. As one Court in the Northern District of California insisted, in severing Does 2-101 and dismissing their cases without prejudice for improper joinder:

> Joining Defendants to resolve what at least superficially appears to be a relatively straightforward case would in fact transform it into a cumbersome procedural albatross. These difficulties would place tremendous burden on Defendants as well. To provide two illustrative examples, each Defendant

> would have the right to be present at every other Defendant's depositions—a thoroughly unmanageable and expensive ordeal. Similarly, *pro se* Defendants, who most likely would not e-file, would be required to serve every other Defendant with a copy of their pleadings and other submissions throughout the pendency of the action at substantial cost. The court . . . cannot permit a case to proceed in this manner.

Pac. Century Int'l, Ltd. v. Does 1-101, 2011 U.S. Dist. LEXIS 124518 (N.D. Cal. Oct. 27, 2011).

To avoid a similar unmanageable maelstrom of litigation, this Court is urged to consider severance.

4. PLAINTIFF MANIPULATES JOINDER TO AVOID PAYING FILING FEES

Plaintiff deviously attempts to join together this large number of defendants under shaky pretenses in order to avoid paying appropriate filing fees. Generally, filing fees serve two purposes. First, they operate as a revenue raising measure to offset the cost to the judicial system for hearing cases. Second, they operate as a minimalistic barrier to bar the filing of utterly frivolous and meritless lawsuits. *See, e.g., In re Diet Drugs*, 325 F. Supp. 2d 540, 541-42 (E.D. Pa. 2004).

Several courts in similar cases involving BitTorrent protocol have also recognized the effect of avoiding filing fees. One Court explained that "these mass copyright infringement cases have emerged as a strong tool for leveraging settlements—a tool whose efficacy is largely derived from the plaintiffs' success in

avoiding the filing fees for multiple suits and gaining early access en masse to the identities of alleged infringers." *Pac. Century Int'l, Ltd. v. Does 1-37*, 2012 U.S. Dist. LEXIS 44368 [*3] (N.D. Ill. Mar. 30, 2012). In the instant litigation, Plaintiff avails himself of the judicial system in something akin to a reverse-class action lawsuit. He avoids paying potentially thousands of dollars in filing fees by spinning the Federal Rules regarding permissive joinder to fit his peculiar set of facts.

IV. CONCLUSION

Defendant has standing as his privacy interests are at stake and the subpoena would trigger an undue burden as well as cause Defendant annoyance and embarrassment. Plaintiff's pursuit by means of a subpoena is not likely to uncover the identity of the copyright infringing person. Given the realities of modern-day Internet connections, an Internet subscriber is hardly certain to be the same person who used that subscriber's IP address to allegedly engage in file-sharing of Plaintiff's work.

In the alternative, the Doe Defendants will very likely raise various defenses under unique factual circumstances. Joinder would be both confusing and unfair to Doe Defendants. Plaintiff fails to meet Rule 20's transactional component for joinder. Even if this Court disagrees, this Court is free to sever on other grounds, especially to promote fundamental concepts of justice and fairness. Thus, the Court

is urged to quash the subpoena directed to Defendant John Doe #25 or, in the alternative, he should be severed from the remaining 29 Defendants and the Complaint against him Dismissed without Prejudice.

Respectfully submitted,

/s Michael Mignogna, Esq.
Michael Mignogna
Bar # 85050
Mattleman, Weinroth & Miller, P.C.
401 Route 70 (Marlton Pike) East, Suite 100
Cherry Hill, NJ 08034
Phone: 856.429.5507
E-mail: mmignogna@mwm-law.com