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

MALIBU MEDIA, LLC.,

Plaintiff,

vs.

JOHN DOE subscriber assigned IP address 69.249.253.94,

Defendant.

_____/

CASE No. 2:14-cv-01280

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

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

I, John Doe, respectfully move the court for dismissal or severance of my case in the above captioned matter and motion to quash the subpoena served on my Internet Service Provider (ISP), Comcast Corporation.

INTRODUCTION:

I have never committed the acts alleged by the plaintiff. After receiving a letter from Comcast Corporation advising me that it had been subpoenaed to release my identity and contact information in this matter, I began to research the plaintiff, Malibu Media, LLC, its affiliates, BitTorrent, and similar cases brought by others. My internet research has revealed that in cases associated with Malibu Media, LLC, when the subpoenaed information is turned over to the plaintiff by the ISP, the defendants, guilty or innocent, received threatening demand letters. These letters typically demand a settlement sum that range from $2500 to $7500, even $13,000 or more in some cases to avoid dealing with lengthy and expensive court battles that can easily bankrupt a working individual. The threats do not end with just letters, in the cases where the ISP provided the

phone numbers of the defendant, persistent (borderline harassing) phone calls are also directed at the defendant, even if they did not commit the alleged act of copyright infringement. While I am respectful of Malibu Media, LLC, or any other company and their right to protect their products and patents, I cannot condone the bullying tactics that other past defendants before me have experienced. I am filing this motion to protect myself from also becoming a victim of these demands; I respectfully request that I be allowed to make this motion anonymously without revealing my personally identifying information as to do otherwise would defeat the purpose of this motion.

ARGUMENT:

I base this motion on six factors: , (1) the person using a device connected to the internet at any given time is not necessarily the individual to whom the involved Internet Protocol address (IP address) is registered, (2) even the Media Access Control (MAC) address will often indicate on the wireless router connected to the internet but cannot be relied upon to determine who accessed the internet at any particular time, (3) the inability to correctly identify who actually accessed the internet through given IP and MAC addresses introduces an unacceptable degree of uncertainty with regard to the identification of actual wrongdoers, (4) improper venue in a recent court ruling: the fact that plaintiff has only been able to show that the geolocation software they use can only provide a location of the alleged infringing IP address; they have not been able to demonstrate how the geolocation software can establish the identity of the defendant, and (5) the investigator, Tobias Fieser, hired by Malibu is not licensed to conduct private detective work and is in potential violation of Pennsylvania's Private Detective Act of 1953.

1. The person using a device connected to the internet at any given time is not necessarily the individual to whom an implicated Internet Protocol IP address) is registered:

There are many circumstances in which the person to whom an Internet Protocol address may be registered is not the only person able to access the internet through that address. These are discussed at length in a Declaration *(Case* 2: *12-cv-02084-MMB Document* 9). A copy of this Declaration is attached. The fact that the person to whom an IP address is registered may not be the only individual who can access the internet through that address and the implications of this have been recognized previously by the courts. In *Case 2:II-cv-03995,* the Honorable Gary Brown noted that "it is no more likely that the subscriber to an IP address carried out a particular computer function-here the purported illegal downloading of a single pornographic film-than to say an individual who pays the telephone bill made a specific telephone call" [p. 6]

2. Even a valid Media Access Control (MAC) address will often only indicate the wireless router connected to the internet and cannot be relied upon to determine who accessed the internet at any particular time:

The identity of devices connected to the internet through an IP address is often limited to the first in a chain of devices. With the advent of the wireless router, often this will be the only device that can be identified. However, ownership of a wireless router, even a secured one, is not tantamount to being the only possible user of the device. Therefore, even the MAC address logged by the Internet Service Provider is of limited and possibly no value in determining who accessed the internet at a given moment or even what computer or other device was used to do so. This is discussed in more detail in the Declaration referenced in (2) above. This has explicitly been recognized in the courts by Judge Gary R. Brown who wrote in RE: BITTORRENT ADULT FILM COPYRIGHT INFRINGEMENT CASES *(Case* 2~JJ~cv-*03995-DRH-GRB Document* 39) that:

> unless the wireless router has been appropriately secured (and in some cases even if it has been secured), neighbors or passersby could access the Internet using the IP address assigned to a particular subscriber and download the plaintiff's film. As one court noted:

> In order to allow multiple computers to access the internet under the same IP address, the cable modem may be connect to a router, or may itself function as a router, which serves as a gateway through which multiple computers could access the internet at the same time under the same IP address. The router could be a wireless device in which case, computers located within 300 feet of the wireless router signal could access the internet through the router and modem under the same IP address. The wireless router strength could be increased beyond 600 feet if additional devices are added. The only way to prevent sharing of the wireless router is to encrypt the signal and even then an individual can bypass the security using publicly available software. [p. 7, citations absent in the original]

3. The inability to identify who actually accessed the internet through implicated IP and MAC addresses introduces an unacceptable degree or uncertainty with regard to the identification or actual wrongdoers.

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 Honorable Gary R. Brown writing on *Case* 2: *ll-cv-03995* (document 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'"). [p. 18]

The Honorable Harold A. Baker noted when commenting on *VPR Internationale v. DOES,' 1-017 (2:11-cv-02068-HAB -DGB # 15),* that:

> Orin Kerr, a professor at George Washington University Law School, noted that whether you're guilty or not, "you look like a suspect."3 Could expedited discovery be used to wrest quick settlements, even from people who have done nothing wrong? The embarrassment of public exposure might be too great, the legal system too daunting and expensive, for some to ask whether VPR has competent evidence to prove its case. In its order denying the motion for expedited discovery, the court noted that until at least one person is served, the court lacks personal jurisdiction over anyone. The court has no jurisdiction over any of the Does at this time; the imprimatur of this court will not be used to advance a "fishing expedition by means of a perversion of the purpose and intent" of class actions. Order, d/e 9. [p. 3]

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, the Honorable 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., Malibu* 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 turn 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. 8]

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 tinest 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).

4. Improper venue: plaintiff has only been able to show that the geolocation software they use can only provide a location of the alleged infringing IP address; they have not been able to demonstrate how the geolocation software can establish the identity of the defendant.

In a recent March 5th, 2014 ruling by the United States District Court in Southern District of Florida, honorable Judge Ursula Ungaro asked the plaintiff to provide convincing evidence that the plaintiff's usage of geolocation or other technologies could establish the identity of the defendant. The final ruling was that an IP address is not a person and cannot adequately identify a BitTorrent pirate, and that the plaintiff's current investigation techniques are not sufficient.

The plaintiff responded in this case: 1:14-cv-20213-UU:

> On March 14, 2014, Plaintiff filed its response to the Court's Order. D.E. 9. Plaintiff has shown that the geolocation software can provide a location for an infringing IP address; however, Plaintiff has not shown how this geolocation software can establish the identity of the Defendant. There is nothing that links the IP address location to the identity of the person actually downloading and viewing Plaintiff's videos, and establishing whether that person lives in this district. For example, when arguing that this IP address is not a coffee shop or open Wi-Fi network, Plaintiff points to the timing of the alleged infringement and the fact that the internet service provider typically provides internet to residences. D.E. 9 at 10. Plaintiff then argues that a coffee shop owner could possibly identify the Defendant. *Id.* Even if this IP ad-

> dress is located within a residence, the geolocation software cannot identify who has access to that residence's computer and who would actually be using it to infringe Plaintiff's copyright. The Court finds that Plaintiff has not established good cause for the Court to reasonably rely on Plaintiff's usage of geolocation to establish the identity of the Defendant. The Court also finds that Plaintiff has not established good cause as to why this action should not be dismissed for improper venue. [p. 1-2]

5. The investigator, Tobias Fieser, hired by Malibu is not licensed to conduct private detective work and is in potential violation of Pennsylvania's Private Detective Act of 1953.

The evidence put forth as the grounds for the copyright claim by plaintiff and their investigator Tobias Fieser is inadmissible. Neither IPP Limited, the company Mr. Fieser works for, nor Mr. Fieser himself is licensed detective agency. Under Section 16.1 of the Pennsylvania Private Detective Act of 1953, any person engaging in the private detective business without a license shall upon conviction be considered guilty of a third degree misdemeanor. To date, extensive internet searches have yielded no actual credentials or proof of competency in past court cases that Mr. Fieser is indeed qualified to perform the investigative work that plaintiff is paying him and IPP Limited to conduct.

Dated: 04/01/2014

Respectfully submitted,

s/John Doe
John Doe
Pro se

CERTIFICATE OF SERVICE

I, John Doe, hereby certify that on 04/01/2014, I forwarded a true and correct copy of Motion to Dismiss and/or Sever Complaint against John Doe and Quash Subpoena Against Same to Christopher P Fiore, Esquire, Fiore and Barber, LLC, 418 Main Street, Harleysville, PA 19438 via US Mail, on:

s/John Doe
John Doe
Pro se