UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE No.1: 12-Civ-21952

FIRST TIME VIDEOS LLC,

Plaintiff,

v.

JOHN DOE,

Defendant.

MOTION TO DISMISS COMPLAINT
AND QUASH SUBPOENA

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

I, John Doe, respectfully move the court for dismissal of my case in the above captioned matter and motion to quash the subpoena served on my Internet Service Provider, Charter Communications.

I have never committed the acts alleged by the plaintiffs. After receiving a letter from Charter Communication advising me that it had been subpoenaed to release my identity and contact information in this matter, I began to research First Time Videos, LLC and similar cases brought by others. My internet research has revealed that in cases associated with First Time Videos, LLC, when the subpoenaed information is turned over to the plaintiffs, the defendants, guilty or innocent, receive demand letters. These letters typically demand from $2500 to $7500 and in some cases in excess of $13000 for settlement to avoid dealing with threatened lawsuits, and the subsequent telephone calls, which have been reported as persistent if not harassing, are the reason I am filing this motion. 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.

I base this motion on four factors: (1) lack of jurisdiction, (2) 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, (3) 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, and (4) the inability to 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.

1. Lack of jurisdiction

The plaintiff has not shown that this Court has jurisdiction over John Doe. It has not been shown that John Doe resides in or committed copyright infringement in the State of Florida, as alleged in the Plaintiff's Complaint. The Plaintiff claims that the court has personal jurisdiction since "geolocation technology" was used to trace the IP address of John Doe to a point of origin within the State of Florida, but fails to offer any proof of such claim. The Plaintiff then suggests that, if John Doe does not live in Florida, the Court still has personal jurisdiction under the Florida long-arm statute because John Doe either downloaded copyrighted content from or uploaded it to Florida residents, yet still fails to offer any proof of such claim. The Plaintiff has provided, in Exhibit A, a list of IP addresses, but in no way has shown that any of those IP addresses have any relation to the State of Florida.

2. 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]

3. Even a valid Media Access Control (MAC) address will often indicate only 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 2-11-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]

4. 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 1-1017 (*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]

Magistrate Judge Harold R. Loyd writing in regard to *Hard Drive Productions v. Does 1-90, C11-03825 HRL* stated:

> Here, plaintiff has failed to allege that its claims against the 90 Doe defendants arise from "a single transaction or a series of closely related transactions." Instead, plaintiff provides a list of all 90 Doe defendants, identified by IP addresses, and the date and time they each appeared in the swarm over a period of63 days. See Complaint, Exh. A. Plaintiff also alleges that each Doe defendant "entered the same exact BitTorrent swarm and "reproduced and distributed the Video to multiple third parties." Complaint ¶29. But, plaintiff's counsel admitted at the hearing **that plaintiff could not truthfully allege that any of the Doe defendants actually transferred pieces of the copyrighted work to or from one another.** [p. 10, emphasis added]

In Case *2:11-cv-03995* which addressed three cases (*Malibu Media, LLC v. John Does 1-26, CV 12-1147 (J..)) (GRB), Malibu Media, LLC v. John Does 1-11, CV 12-1150(LDW) (GRB),* and *Patrick Collins, Inc. 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 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. 8]

Finally, also writing in case 2:11-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 finest 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).

It is for these reasons that I ask the Court to dismiss this complaint and quash the subpoena for identifying and contact information served on Charter Communications for me, John Doe.

Dated: 7/16/2012

Respectfully submitted,

/s/John Doe
John Doe
Pro se

CERTIFICATE OF SERVICE

I, John Doe, hereby certify that on July 16, 2012, I forwarded a true and correct copy of Motion to Dismiss Complaint Against John Doe and Quash Subpoena Against Same to Joseph Perea, Joseph Perea, P.A.; 9100 S Dadeland Blvd, Suite 1500, Miami, Florida 33156 by United States first class mail.

/s/John Doe
John Doe
Pro se