

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

MALIBU MEDIA, LLC
Plaintiff,

v.

Case No. 8:12-cv-669-T23-AEP

JOHN DOES 1-25,
Defendants.

**JOHN DOE 25 MOTION TO SEVER, DISMISS, OR ISSUE PROTECTIVE ORDER,
AND SUPPORTING MEMORANDUM OF LAW**

John Doe 25, identified by the IP addresses 173.78.82.100, by and through undersigned counsel file this Motion and move this Court to: sever and dismiss the Defendants and/or issue a protective order in connection with the subpoena directed at the ISP (here Verizon) and object to the discovery sought. This Court should grant the relief requested. In support, Defendants submit this Memorandum of Law.¹

INTRODUCTION

Plaintiff, a pornographic film production company, has launched a massive litigation vanguard throughout the country and in this District, led by attorney M. Keith Lipscomb of Miami. Until recently, Mr. Lipscomb has been content to utilize the Florida state procedural device of the “pure bill of discovery” on behalf of porno companies in dozens of actions seeking to identify tens of thousands of “Doe” defendants. His modus operandii is simple: (1) obtain a long list of IP addresses harvested by questionable (and possibly illegal) means relating to one or more pornographic films owed by Plaintiff; (2) file a single suit (with a single

¹ Doe 25 acknowledges and joins the arguments already filed in this matter by Does 3, 6 and 24. See Dkt.

\$350 filing fee); (3) obtain an ex parte order to allow for jurisdictional discovery from the Internet Service Providers for the IP addresses harvested; (4) subpoena the records from the ISPs; (5) wait; (6) upon receipt of the contact information for the ISP account holders, send demand letters seeking a few thousand dollars; (7) collect the money from frightened Does in ; (8) to the extent any Doe resists, threaten further action; (9) file individual suits to scare Does of the possibility; (10) settle for any amount to move on to the next case. This business model is the Florida flavor of what has become known as “copyright troll” litigation.

Late last year, the BitTorrent game moved to federal court. Instead of relying exclusively on the pure bill of discovery tool in cases involving thousands of potential defendants per case, the Plaintiffs found success obtaining ex parte preliminary discovery orders from federal magistrate judges. The fox was in the hen house. Once the ISP subpoenas are issued, the result is similar – the ISPs send out letters to their subscribers, and the subscribers (i) do nothing (and Plaintiff gets their information); (ii) contact Plaintiff (and reveal their information); (iii) object pro se (and possibly reveal their information); (iv) object through counsel. If there is an objection, the case is dismissed unilaterally by the Plaintiff, or if money is paid, settled and dismissed. The financial result is also the same as in state court – persons desperate to avoid the permanent taint of having their name associated with explicit pornography titles simply settle.

It is also important to note that there are no cases of record where a Plaintiff in a BitTorrent case has gone into post-CMR discovery against a defendant, or faced any real discovery. These cases do not exist to be contested, tried, or otherwise decided on the merits. They are simply a means of extorting a lowball settlement from a nominal defendant, regardless of guilt or innocence, meritorious defenses, or anything other than a cost-benefit

analysis by a threatened defendant. It is little wonder why this business method is being employed by the porno copyright owners.

To his credit, Mr. Lipscomb has learned and evolved his methods as a result of the mistakes of others, specifically copyright troll attorney extraordinaire Jeff Weaver of Dunlap, Grubb & Weaver. DGW, the national leader in Doe BitTorrent cases, has filed hundreds of cases against tens of thousands of Doe defendants, without regard to personal jurisdiction. Mr. Lipscomb fashions his complaints to specifically state that the purported basis for jurisdiction is the physical address associated with the IP address of the various Does, present in the State. More on that later. He keeps the number of Does in any particular complaint low, and has avoided filing the cases with thousands of Does to escape additional scrutiny from the bench. Add to that the fact that he files cases simultaneously in clumps, thereby avoiding having any one judge pull a number of cases off the wheel at the same time, and evading potential questions being raised by a common judge with several cases before them, and the gamesmanship becomes more evident.

In 2012, as of this case's filing, Mr. Lipscomb had filed 22 such federal copyright actions against 481 Does in the Middle District. Only 34 copyright infringement cases *total* have been filed in the Middle District this year. In 2011, his office mate Mr. Alexander Liam filed 11 such federal copyright actions against 105 Does, out of a *total* of 37 copyright infringement cases in the Middle District. None of these actions has moved beyond the common preliminary discovery phase, with nearly all of the Does dismissed and settlements obtained. In June, 2012, this very Plaintiff filed eight additional lawsuits in the Middle District, all precisely the same cookie cutter BitTorrent lawsuit brought by Mr. Lipscomb.

In 2012, again as of the date of filing of this suit, Malibu Media LLC had filed 116

lawsuits in 11 district courts against 2,095 Doe defendants. Of these, exactly three persons are individually identified by name.

PROCEDURAL BACKGROUND

Plaintiff, Malibu Media, LLC, is a California corporation and professes to have its principal place of business in California. (Complaint [Dkt. 1] ¶ 6.) Plaintiff neither alleges nor appears to transact business in or have any identifiable connections to Florida. (*See generally* Compl.) Plaintiff claims to be the copyright holder of a trove of more than 100 pornographic videos alleged to be downloaded, only a portion of which have had copyrights registered. In this lawsuit, Plaintiff alleges that twenty five (25) “John Doe” Defendants² are liable for the infringement and contributory infringement of Plaintiff’s copyright in a supposed “site rip”. (*See generally* Dkt. 1) Plaintiff uses IP addresses, numbers assigned by an Internet Service Provider (ISP) to each subscriber, to allegedly identify these John Doe Defendants. Astonishingly, Plaintiff acknowledges that the basis for the identification is a single data point, which does not identify the start time, end time, duration, or otherwise identify an alleged downloader other than an IP address.

On May 29, 2012, Plaintiff filed an *ex parte* Motion for Leave to Serve Third Party Subpoenas Prior to a Rule 26(f) Conference (“Motion for Expedited Discovery”) seeking leave from the Middle District of Florida to issue subpoenas directed at each Defendants’ ISP seeking the Defendants’ personally identifying information. (*See* Mot. for Exp. Disc. [Dkt. 4].) The Magistrate Judge granted Plaintiff’s *ex parte* Motion for Expedited Discovery the next day. (*See* Order Granting Mot. for Exp. Disc. [Dkt. 5].)

Plaintiff then caused a subpoena directed at Verizon to be issued from the United States

² The CM/ECF system incorrectly captions the Defendants “Does 1-99”(stet.).

Court for the Northern District of Texas seeking the personally identifying information of John Does 21-25 (the “Subpoena”). (See Exhibit “A”, a true and correct copy of the Subpoena which is incorporated by reference herein at if set forth verbatim herein.) Defendants have filed motions to thwart the discovery [Dkt. 12; Dkt. 13; Dkt. 15].

ARGUMENT

John Doe 25 adopts and incorporates by reference in their entirety the arguments presented by the other Does in its Motion. Rather than reiterate them in full, they are summarized as follows:

A. John Doe Defendants 2-25 Should be Severed and Dismissed from this Case due to Misjoinder

The joinder of these Defendants is improper under Fed. R. Civ. P. 20(a) and (b). *AF Holdings, LLC v. Does 1-97*, No. C-11-3067-CW(DMR), slip op., 2011 WL 2912909, at *2 (N.D. Cal. July 20, 2011) (quoting *Coughlin v. Rogers*, 130 F.3d 1348, 1350 (9th Cir. 1997)).

1. Plaintiff’s Claims do Not Arise Out of “the Same Transaction, Occurrence, or Series of Transactions or Occurrences”

Mere alleged use of a BitTorrent protocol is insufficient to sustain permissive joinder, both in the Eleventh Circuit³ and beyond.⁴ *Liberty Media Holdings, LLC v. BitTorrent Swarm*, 277 F.R.D. 672, 675 (S.D. Fla. 2011) (quoting *Hard Drive Prods., Inc. v. Does 1-188*, 809 F.

³ See, e.g., *Patrick Collins, Inc. v. Does 1-16*, No. 6:12-cv-477-ACC-KRS, Order to Show Cause [Doc. No. 7] (M.D. Fla. Apr. 5, 2012) (plaintiff later voluntarily dismissed case); *Liberty Media Holdings, LLC v. BitTorrent Swarm*, 277 F.R.D. 672 (S.D. Fla. 2011) (severing defendants); *Liberty Media Holdings, LLC v. BitTorrent Swarm*, 277 F.D.R. 669 (S.D. Fla. 2011) (severing defendants); *Raw Films, Inc. v. Does 1-32*, No. 1:11-CV-2939, slip op., 2011 WL 6840590 (N.D. Ga. Dec. 29, 2011) (order severing defendants); *Patrick Collins, Inc. v. Does 1-35*, No. 1:11-CV-02940 (N.D. Ga. Dec. 19, 2011) (order severing defendants); *K-Beech, Inc. v. Does 1-63*, No. 1:11-CV-2941-CAP (N.D. Ga. Dec. 5, 2011) (order severing defendants).

⁴ See, e.g., *Third Degree Films v. Does 1-3577*, No. C11-02768 LB, slip op., 2011 WL 5374569 (N.D. Cal. Nov. 4, 2011); *Hard Drive Productions, Inc. v. Does 1-30*, No. 2:11-CV-345, slip op., 2011 WL 4915551 (E.D. Va. Oct. 17, 2011) (severing defendants); *K-Beech, Inc. v. Does 1-78*, No. 5:11-CV-05060 (E.D. Penn. Oct. 3, 2011) (order severing defendants).

Supp. 2d. 1150, 1164 (N.D. Cal. Aug. 23, 2011)). *In re: BitTorrent Adult Film Copyright Infringement Cases*, No. 2:11-cv-3995-DRH-GRB, 2012 WL 1570765, at *11 (E.D.N.Y. May 1, 2012).

Many courts, including the Middle District of Florida, have reasoned that John Doe defendants in analogous lawsuits were improperly joined based on the time span between each defendant's alleged sharing of the file. *Patrick Collins, Inc. v. Does 1-16*, No. 6:12-cv-477-ACC-KRS, Order to Show Cause [Doc. No. 7] (M.D. Fla. Apr. 5, 2012) (ordering plaintiff to show cause why defendants should not be severed when "access occurred on different dates"); *Raw Films, Inc. v. Does 1-32*, No. 1:11-CV-2939-TWT, slip. op., 2011 WL 6840590, at *2 (N.D. Ga. Dec. 29, 2011) (time span of more than 4 months); *K-Beech, Inc. v. Does 1-63*, No. 1:11-CV-02941-CAP, at 6 (N.D. Ga. Dec. 5, 2011) (time span of almost 3 months); *Liberty Media Holdings, LLC*, 277 F.R.D. at 675 (time span of 2 months); *Liberty Media Holdings, LLC v. BitTorrent Swarm*, 277 F.R.D. at 671 (time span of 2 months); *Hard Drive Prods., Inc.*, 809 F. Supp. 2d 1150, 1163 (time span of 6 weeks). *Patrick Collins, Inc. v. Does 1-16*, *Id.* at *1 (citations omitted).

In *Raw Films, Inc.*, the court found that "[d]ownloading a work as part of a swarm does not constitute 'acting in concert' with one another, particularly when the transactions happen over a long period." 2011 WL 6840590, at *2; *see also K-Beech, Inc.*, No. 1:11-CV-02941-CAP, at 4 (N.D. Ga. Dec. 5, 2011) (order granting motion to sever); *see also K-Beech, Inc.*, No. 1:11-CV-02941-CAP, at 5-6 (N.D. Ga. Dec. 5, 2011). *See, e.g., MCGIP, LLC v. Does 1-149*, No. C 11-02331 LB, slip op., 2011 WL 4352110, at *3 (N.D. Cal. Sept. 16, 2011) (finding misjoinder where the plaintiff failed to show that any of the defendants actually exchanged any piece of the seed file with one another); *Boy Racer, Inc. v. Does 1-60*, No. C 11-01738 SI, slip

op., 2011 WL 3652521, at *4 (N.D. Cal. Aug. 19, 2011) (finding misjoinder because “Plaintiff [did] not plead facts showing that any particular defendant illegally shared plaintiff’s work with any other particular defendant”). Plaintiff’s allegations that Defendants committed the same type of violation in the same way simply does not equate to participation in the same transaction, occurrence, or series of transaction or occurrence. *See LaFace Records, LLC v. Does 1-38*, No. 5:07-CV-298-BR, 2008 WL 544992, at *7 (E.D.N.C. Feb. 27, 2008). This basis alone is sufficient to warrant the severance of the Defendants.

2. Joinder will Result in a Lack of Judicial Economy and Prejudice the Defendants Moving Forward

“Among the factors to be considered by the court in exercising its discretion under Rule 21 are whether ... judicial economy would be facilitated, whether prejudice would be avoided if severance were granted, and whether different witnesses and documentary proof are required for the separate claims.” *Hartley v. Clark*, No. 3:09cv559/RV/EMT, 2010 WL 1187880, at *4 (N.D. Fla. Feb. 12, 2010); *see also*, 7 Charles Alan Wright, et al., *Federal Practice and Procedure* § 1652, at 396 (3d ed. 2001) (“[T]he court has discretion to deny joinder if it determines that the addition of the party under Rule 20 will not foster the objective of the rule, but will result in prejudice, expense or delay”).

3. Plaintiff’s Abusive Litigation Tactics Deprives the Court of Related Filing Fees

The Court needs to appreciate the scope of abuse this fox in the henhouse poses. First, copyright actions themselves have made up a tiny percentage of the cases brought in this district. Since 1989, cases designated as copyright infringement actions have averaged 34 per

year (high 62 (2002), low 10 (1989)).⁵ Only a handful of “Doe” defendant cases were brought in the previous twenty years. In 2011, 16 “Doe” BitTorrent actions were filed. Of those, all but two have been closed. In the two remaining cases, two defendants remain in one, and in the other, the Court is in the process of dismissing numerous defendants and granting numerous motions to quash in the other.

In 2012, to date, Mr. Lipscomb filed 22 such federal copyright actions against 481 Does in the Middle District. Only 34 copyright infringement cases *total* have been filed in the Middle District this year. In 2011, his office mate Mr. Alexander Liam filed 11 such federal copyright actions against 105 Does, out of a *total* of 37 copyright infringement cases in the Middle District. None of these actions has moved beyond the common preliminary discovery phase, with nearly all of the Does dismissed and settlements obtained. Earlier this month, this very Plaintiff filed eight additional lawsuits in the Middle District, all precisely the same cookie cutter BitTorrent lawsuit brought by Mr. Lipscomb.

In 2012, to date, Malibu Media LLC has filed 116 lawsuits across the country – in 11 district courts against 2,095 Doe defendants. Of these, exactly three persons are individually identified by name. Plaintiff’s improper joinder tactics rob the court of the fees it requires to adjudicate such actions. Mr. Lipscomb’s firm and an associated solo practitioner practicing out of his office (Alexander Liam) were responsible for filing nearly all of these cases. Dunlap, Grubb & Weaver (Jeff Weaver) were the pioneers in BitTorrent prosecution, having named tens of thousands of Does nationwide, but have only filed a precious few Doe cases in Florida, and a handful of post-Doe individual actions.

In a similar case, the Northern District of Illinois recognized that “the plaintiffs’ tactics

⁵ See Exhibit A.

deny the federal courts additional revenue from filing fees in the suits that should be filed to obtain the information the plaintiffs desire.” *CP Prods.*, 2011 WL 737761, at *1 (“No predicate has been shown for thus combining 300 separate actions on the cheap – if CP had sued the 300 claimed infringers separately for their discrete infringements, the filing fees along would have aggregated \$105,000 rather than \$350.”) *Pacific Century Int’l, LTD v. Does 1-37*, No. 1:12-cv-01057 (consolidated action), 2012 WL 1072312, at *5 n.15 (N.D. Ill. Mar. 30, 2012). This was also recognized and discussed in great detail in an analogous case in the Eastern District of New York, *In re Diet Drugs*, 325 F. Supp. 2d 540, 541-42 (E.D. Pa. 2004); *see also In re Seroquel Prods. Liability Litig.*, 2007 WL 737589, at *2-3 (M.D. Fla. Mar. 7, 2007) (denying reduction of filing fees, noting the burden on the court and the “gatekeeping feature of a filing fee”).

Several courts in similar cases involving BitTorrent protocol have also recognized the effect of a countenancing a single filing fee. One court described the “common arc of the plaintiffs’ litigation tactics” in these cases:

...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.

Pacific Century, 2012 WL 1072312, at *3. Thus, the plaintiffs file a single case, and pay one filing fee, to limit their expenses as against the amount of settlements they are able to negotiate. Postponing a determination on joinder in these cases “results in lost revenue of perhaps millions of dollars (from lost filing fees) and only encourages plaintiffs in copyright actions to join (or misjoin) as many doe defendants as possible.” *K-Beech, Inc. v. John Does 1-41*, 2012 WL 773683, at *5 (S.D. Tex. 2012).

In the four cases before this Court, plaintiffs have improperly avoided more than

\$25,000 in filing fees by employing its swarm joinder theory. Considering all the cases filed by just these three plaintiffs in this district, more than \$100,000 in filing fees have been evaded. If the reported estimates that hundreds of thousands of such defendants have been sued nationwide, plaintiffs in similar actions may be evading millions of dollars in filing fees annually. Nationwide, these plaintiffs have availed themselves of the resources of the court system on a scale rarely seen. It seems improper that they should profit without paying statutorily required fees.

In re: BitTorrent Adult Film Copyright Infringement Cases, 2012 WL 1570765, at *13.

Here, Plaintiff should be required to attack each Doe on its own merits, and the case should be dismissed for improper joinder. By foregoing the real cost of litigation by naming a host of additional defendants, Plaintiff leverages its “investment” in the business model. If \$350 can obtain a \$2800 settlement (the cost of eight additional filing fees) against one person, paying a single filing fee against ten defendants can yield \$28,000 in settlements under this business model. This abuse of the system robs the court of \$2800 in one case alone. Plaintiff has filed more than a hundred this year. [Exhibit A].

4. Additional costs are likely.

Further, if this case proceeds, Plaintiff is likely to make further discovery requests against each individual Defendant that will further increase complexity and cost. This is the exact situation in which the Northern District of California found itself when it failed to sever the defendants in a similar case:

[Plaintiff] would require nothing less than an inspection of the subscriber’s electronically stored information and tangible things, including each of the subscriber’s computer and computers of those sharing his internet network. . . . Presumably, every desktop, laptop, smartphone, and tablet in the subscriber’s residence, and perhaps any residence of any neighbor, houseguest or other sharing his internet access, would be fair game. Beyond such an inspection, [Plaintiff] might require still more discovery, including interrogatories, document requests and even depositions.

Boy Racer, Inc. v. Does 1-52, No. 11-CV-2329-PSG, at 4 (N.D. Cal. Sept. 13, 2011) (order denying further discovery). The courthouse circus which will likely ensue if the Defendants are

not severed will result in economic prejudice to the Defendants moving forward. *See, e.g., Bridgeport Music, Inc. v. IIC Music*, 202 F.R.D. 229, 233 (M.D. Tenn. 2001) (“If joined in one action, hundreds of Defendants will be subject to an overwhelming onslaught of materials and information unrelated to the specific claims against them – all of which they must pay their attorneys to review”). To prevent prejudicing the Defendants and maximize judicial economy, this Court should sever and dismiss the all but the first Defendant from this case.

B. This Court Should Issue a Protective Order Preventing or Limiting the Disclosure of the John Does Personally Identifying Information by Verizon

Although Federal Rule of Civil Procedure 45(c) indicates that a Motion to Quash be filed in the district court for the district that issued the Subpoena, it does not alter the general rule that the broad outlines of discovery in a civil case are to be controlled by the court in which the case is filed. *Straily v. UBS Fin. Servs., Inc.*, No. 07-cv-884-REB-KMT, 2008 WL 5378148, at *2 (D. Colo. Dec. 23, 2008); *Wells v. GC Servs. LP*, No. C06-03511 RMW HRL, 2007 WL 1068222, at *1 (N.D. Cal. Apr. 10, 2007); *Manufacturer Direct, LLC v. Directbuy, Inc.*, No. 2:05-cv-451, 2007 WL 496382, at *2-3 (N.D. Ind. Feb. 12, 2007); *Platinum Air Charters, LLC v. Aviation Ventures, Inc.*, No. 2:05-cv-01451-RCJ-LRL, 2007 WL 121674, at *3 (D. Nev. Jan. 10, 2007); *Best Western Int’l, Inc. v. Doe*, No. cv-06-1537-PHX-DGC, 2006 WL 2091695, at *2 (D. Ariz. July 25, 2006); *Static Control Components, Inc. v. Darkprint Imaging*, 201 F.R.D. 431, 434 (M.D.N.C. 2001) (district where case was pending had authority to issue protective order, pursuant to its right to control general outline of discovery, even though the particular discovery dispute arose from subpoena issued in another district) (citing *Fincher v. Keller Indus., Inc.*, 129 F.R.D. 123, 125 (M.D.N.C. 1990)); *Pilcher v. Direct Equity Lending*, No. 99-1245-JTM, 2000 WL 33170865, at *4 n.8 (D. Kan. Dec. 22, 2000) (“Under

Rule 26(c), the court in which the action is pending . . . has jurisdiction to issue a protective order limiting discovery”). A party’s “discovery rights [in other districts] can rise no higher than their level in the district of trial.” *Fincher*, 129 F.R.D. at 125. As such, this Court possesses the authority to both hear and grant the relief requested in the John Doe’s motion for a Rule 26 and/or 30(d) protective order to prohibit or limit discovery of their personally identifying information. Fed. R. Civ. P. 26(c)(1) (“a party may move for a protective order in the court where the action is pending”); Fed. R. Civ. P. 30(d)(3)(1) (“The motion may be filed in the court where the action is pending”).

1. A Protective Order Should Be Issued Because the Information Sought by the Subpoena is Irrelevant

“The foremost fundamental principle regarding subpoenaed discovery is that a subpoena duces tecum to obtain materials in advance of trial should be issued only when the party seeking the materials can show that the materials are evidentiary and relevant.” *Straily v. UBS Fin. Servs., Inc.*, No. 07-cv-884-REB-KMT, 2008 WL 5378148, at *1 (D. Colo. Dec. 23, 2008); 81 Am. Jur. 2d *Witnesses* § 20. As protective order may properly be issued to when a subpoena seeks irrelevant information. *See Auto-Owners Ins. Co. v. Southeast Floating Docks, Inc.*, 231 F.R.D. 426, 429 (M.D. Fla. 2005); *cf.* Fed. R. Civ. P. 26(b). The term “relevant” as used in Rule 26 is broad, but not exhaustive. While matters which may aid a party in the preparation or presentation of its case are relevant, matters without bearing either as direct evidence or as leads to evidence are not within the scope of inquiry. *See Lewis v. United Air Lines Transp. Corp.*, 27 F.Supp. 946 (D. Conn. 1939). As the Subpoena here was issued prior to the Rule 26(f) conference, the relevancy of the discovery sought should be even more narrowly tailored to that information which is necessary to definitely and immediately allow Plaintiff to proceed with this lawsuit. Here, the subpoenaed information will not allow Plaintiff

to identify the individuals responsible for infringing its copyright and who could properly be named as Defendants in this lawsuit.

The discovery requested through Plaintiff's Subpoena is based on the faulty assumption that the Internet subscribers identified in Exhibit A to the Complaint are the individuals who actually infringed Plaintiff's copyright. However, Plaintiff admits that the only individual that can be identified through an IP address is an ISP subscriber. (Decl. of Tobias Fieser [Doc. No. 3-2] ¶¶ 8-9.) Many courts have recognized that "the ISP subscribers to whom a certain IP address was assigned may not be the same person who used the Internet connection for illicit purposes." *SBO Pictures, Inc. v. Does 1-3036*, No. 11-4220 SC, 2011 WL 6002620, at *3 (N.D. Cal. Nov. 30, 2011); *e.g. In re: Ingenuity 13 LLC*, No. 2:11-mc-0084-JAM-DAD, Order [Doc. No. 24], at *10 (E.D. Cal. Mar. 21, 2012) ("the identities of the subscribers associated with the identified IP addresses ... would not reveal who actually downloaded petitioner's work, since the subscriber's internet connection could have been used by another person at the subscriber's location, or by an unknown party who obtained access to the subscriber's internet connection without authorization"); *Hard Drive Productions, Inc. v. Does 1-130*, No. C-11-3826-DMR, 2011 WL 553960, at *2 (N.D. Cal., Nov. 16 2011) ("Plaintiff concedes, in some cases the Subscriber and the Doe Defendant will not be the same individual"); *Pac. Century Int'l Ltd. v. Does 1-101*, No. C-11-02533-DMR, 2011 WL 5117424, at *2 (N.D. Cal. Oct. 27, 2011).

An IP address provides only the location at which one of any number of computer devices may be deployed, especially when used with a wireless router.⁶ The United States

⁶ "What is an IP address?" available at <http://computer.howstuffworks.com/internet/basics/question5492.htm>. Thus, it is even less likely that an ISP subscriber (e.g. a John Doe) carried out a particular computer function than that an individual who pays a home telephone bill made a specific call.

District Court for the Eastern District of New York noted that:

If you only connect one computer to the Internet, that computer can use the address from your ISP. Many homes today, though, use routers to share a single Internet connection between multiple computers. Wireless routers have become especially popular in recent years, avoiding the need to run network cables between rooms. If you use a router to share an Internet connection, the router gets the IP address issued directly from the ISP. Then, it creates and manages a subnet for all the computers connected to that router.

In re: BitTorrent Adult Film Copyright Infringement Cases, 2012 WL 1570765, at *3 (quoting *Illustrating this fact, the court in VPR International v. Does 1-1017*, 2:11-cv-02068-HAB-DGB (C.D. Ill. Apr. 29, 2011) cited an instance involving 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 ISP subscribers' Wi-Fi connections (including a secure connection from the State University of New York).

Id. at 2 (citing Carolyn Thompson, *Bizarre Pornography Raid Underscores Wi-Fi Privacy Risks* (April 25, 2011), http://www.msnbc.msn.com/id/42740201/ns/technology_and_science-wireless/).

These circumstances create serious doubt as to Plaintiff's claim that the expedited discovery sought will produce information sufficient to identify the individuals who actually infringed upon Plaintiff's copyright. 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;

It is possible that any family member living in that household, or visitor of that household, could have performed the complained of infringement. Unless the wireless router had been appropriately secured (and that security had not been compromised), neighbors or a passersby could assess the Internet using the IP address assigned to a particular subscriber and download Plaintiff's film.

Plaintiff's counsel estimated that 30% of the names turned over by ISPs are not those of the individuals who actually downloaded or shared copyrighted material.

Digital Sin, Inc. v. Does 1-176, --F.R.D.--, 2012 WL 263491, at *3 (S.D.N.Y. Jan. 30, 2012)

(emphasis added); also *SBO Pictures*, 2011 WL 6002620, at *3. In a denying expedited

discovery in a similar case, the Eastern District of California noted:

Although the revised Hansmeier declaration clarifies that he observed the co-conspirators' IP addresses engaged in the same downloading and uploading as John Doe, the declaration still does not establish that none of the internet subscribers whose information plaintiff seeks to obtain are innocent internet users. The concern remains that potentially non-offending users' information is being sought... Because plaintiff seeks information about the "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 innocent internet users into the litigation, placing a burden upon them that weighs against allowing the discovery as designed.'" *Id.* (quoting *Hard Drive Prods.*, 2011 WL 5573960, at *2).

First Time Videos, LLC v. Doe, No. 2:11-cv-3478-GEB-EFB, 2012 WL 423714, at *5 (E.D.

Cal. Dec. 30, 2011).

Further, studies have shown that the type of tracking software used by investigators, such as IPP International, to identify BitTorrent users often produces a large number of false positive IP hits. One study performed by the Department of Computer Science and Engineering at the University of Washington determined that "copyright holders utilize inconclusive methods for identifying infringing BitTorrent users. [The Researchers] were able to generate hundreds of DMCA takedown notices for machines under [their] control at the University of Washington that were not downloading or sharing any content." Michael Piatek et al., *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 2008, (July 29, 2008) http://www.usenix.org/event/hotsec08/tech/full_papers/piatek/piatek.pdf.

Specifically, the article concludes:

[W]e find that it is possible for a malicious user (or buggy software) to implicate (frame) seemingly any network endpoint in the sharing of copyrighted materials. We have applied these techniques to frame networked printers, a wireless (non-NAT) access point, and an innocent desktop computer, all of which have since received DMCA takedown notices but none of which actually participated in any P2P networks.

Id.

Accordingly, the information sought by Plaintiff regarding the identity of the John Does is irrelevant to this lawsuit based on inaccuracy of the tracking software and the fact that many individuals will often access the Internet through the same ISP account. As such, this Court should issue a protective order preventing or limiting the disclosure of the John Doe's personally identifying information by Verizon.

C. Plaintiffs Rely on Illegal Private Investigators to Obtain IP Addresses

Finally, the court should take note of the fact that Plaintiff relies on the affidavit of a German company's representative to establish a factual predicate for suit. The problem with this activity is that it is a misdemeanor in Florida to engage in "private investigation" without a license. Fla. Stat. 493.6120(1).⁷ Florida defines "private investigation" as "any individual who, for consideration, advertises as providing or performs private investigation. This does not include an informant who, on a one-time or limited basis, as a result of a unique expertise, ability, vocation, or special access and who, under the direction and control of a Class "C" licensee or a Class "MA" licensee, provides information or services that would otherwise be included in the definition of private investigation." Fla. Stat. 493.6101 (16). "Private investigation" includes: "(b) The identity, habits, conduct, movements, whereabouts, affiliations, associations, transactions, reputation, or character of any society, person, or group of persons"; "(f) The causes and origin of, or responsibility for, fires, libels, slanders, losses,

⁷ "(1) Any person who violates any provision of this chapter except [s. 493.6405](#) commits a misdemeanor of the first degree, punishable as provided in [s. 775.082](#) or [s. 775.083](#)."

accidents, damage, or injuries to real or personal property”; and “(g) The business of securing evidence to be used before investigating committees or boards of award or arbitration or in the trial of civil or criminal cases and the preparation therefor.” Private investigators have an extensive initial application process (493.6105), and must “(f) Be a citizen or permanent legal resident alien of the United States or have appropriate authorization issued by the United States Citizenship and Immigration Services of the United States Department of Homeland Security.” 493.6106.

In other words, Fieser is the only person who can testify regarding this case. For his part, Mr. Tobias Fieser, the Plaintiff’s star declarant, acknowledges that he was “tasked by IPP with implementing, monitoring, analyzing, reviewing, and attesting to the results of the investigation” [Para. 13]. Mr. Fieser also “correctly installed and initiated [IPP] on a server in the United States.”[15] He “personally extracted the resulting data” [16], “isolated the transactions and the IP addresses” [17], and after further “analysis” Fieser himself declares that he “viewed the Movie side-by-side with the digital media file identified by the hash value set forth in Exhibit B and determined that the digital media file contained a movie that was identical, strikingly similar, or substantially similar.” [22]

Mr. Fieser places great emphasis on the importance of validating the “Works” by control copy against the digital media file identified by a hash tag. There is no corresponding statement about whether any of the Does downloaded what constituent movies, what portions of the site rip, one single 2MB file, or many. There is no statement about the verification of the hash codes on any of the pieces, how many of them were logged, or anything particular about these alleged Doe transactions whatsoever. Given the flimsy nature of the allegation and the purported volume of materials (more than 100+ constituent movies, only a portion of which

are registered with the Copyright Office) it is extraordinary for its gaping holes in evidentiary support.

To analogize, Mr. Fieser is saying “these 25 people stole the victim’s car, identified by this VIN [40-digit SHA-1 hash code]. I looked at a control copy of the car, and these are the same.” What he is pointedly not saying is whether the car and the 25 examples were the whole car (identified by the VIN) or 117 pieces of the car, separately identified as a part of the car (by VIN) and identified by their own individual hash. He does not identify where in the United States the server is located (much less if it is in the State of Florida or within this district).

The process by which the identification of the infringing material on the internet is problematic. The steps from the IPTRACKER software manual (excerpted from Exhibit A to Fieser’s declaration) are:

1. Download the Data [from where?], verify and allocate definitively to Rights holder. [2.1.1]
2. Use hash value to search for lists of potential sources on the internet by IP address. [Find potential infringing copies of file in the wild]
3. Download lists from those servers sequentially.
4. Make file request via P2P network.
5. If the request is honored, the download is started, and either partially or fully completed.

This means that their factual predicate for suit is established by Plaintiff’s own downloading of their own movie from the real culprits, the infringing *websites*. Plaintiff is infringing on itself to provide itself with the purported evidence it needs to make a claim against individuals. There may not be a remedy for every wrong.

CONCLUSION

For the reasons stated, this case is the tip of the proverbial iceberg. And Winter is Coming. The pattern here signals a vast increase in this type of litigation in this district. It is designed to avoid judicial review and allow asymmetric exploitation of innocent victims of computer hacking, without judicial oversight. The court should grant the relief requested and quash the subpoena, at a minimum.

DATED this 23rd day of July, 2012.

LAW OFFICES OF BRADFORD A.
PATRICK PA

/s/ Bradford A. Patrick
Bradford A. Patrick, Esq.
Florida Bar No.: 529850
3001 North Rocky Point Dr. East, Suite 200
Tampa, Florida 33607
Telephone: (813) 384-8548
Facsimile: (813) 333-7321
E-mail: bap@baplegal.com
Attorney for Doe 25

CERTIFICATE OF COMPLIANCE WITH LOCAL RULE 3.01(G)

Plaintiff and Defendants have conferred and Plaintiff does not consent to the relief requested.

CERTIFICATE OF SERVICE

I certify that on July 23, 2012, I electronically filed the foregoing with the Clerk of the Court by using the *CM/ECF* system for the Service List below.

/s/ BRADFORD A. PATRICK

SERVICE LIST

VIA ECF:

M. Keith Lipscomb
Lipscomb, Eisenberg & Baker, PL
Penthouse 3800
2 South Biscayne Blvd.
Miami, FL 33131
786/431-2228
Fax: 786/431-2229
Email: klipscomb@lebfirm.com

Katie Lee Dearing
The Dearing Law Firm, P.A.
Suite 500
500 West Adams Street
Jacksonville, FL 32202
904/355-8001
Fax: 904/355-8088
Email: katie@dearingfirm.com

William R. Wohlsifer
William R. Wohlsifer, PA
Suite B
1100 E Park Ave
Tallahassee, FL 32301
850/219-8888
Fax: 866/829-8174
Email: william@wohlsifer.com

Jerome W. Hoffman
Holland & Knight, LLP
315 S Calhoun St - Ste 600
PO Drawer 810
Tallahassee, FL 32302
850/425-5654
Fax: 850-224-8832
Email: jerome.hoffman@hklaw.com