UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

MALIBU MEDIA, LLC.	)	
	)	
Plaintiff,	)	Case No: 8:12-cv-01420-JDW-TGW
	)	
v.	)	
	)	
JOHN DOES 1-15,	)	
	)	
Defendants.	)	
	)	

PLAINTIFF'S MEMORANDUM IN OPPOSITION TO JOHN DOE 1'S MOTION TO SEVER, DISMISS, OR ISSUE PROTECTIVE ORDER [DKT. #8]

I. INTRODUCTION

Defendant John Doe 1's Motion to Sever, Dismiss, Or Issue Protective Order ("Motion") should be denied. Defendant's goal is to discredit both Plaintiff and Plaintiff's counsel so as to distract this Court from Defendant's infringement and Plaintiff's valid and proper copyright claim.

Courts in the Eleventh Circuit have acknowledged that the tactics used by Defendant are nothing more than ad hominem attacks. "The only argument remaining—that copyright infringement suits of this sort are baseless 'fishing expeditions' used solely to extort money from alleged infringers—amounts to nothing more than an *ad hominem* attack on the Plaintiff. This line of argument fails to persuade." AF Holdings, LLC v. Does 1-162, 11-23036-CIV, 2012 WL 488217 at *1 (S.D. Fla. Feb. 14, 2012). Defendant's Motion particularly rings true to this by personally attacking undersigned without basis or reason.

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

online theft of Plaintiff's property greatly damages its business, products, and reputation. At this stage of the litigation process, Plaintiff has no other option but to file suit against the owners of these IP addresses to obtain the infringer's identities. If this Court were to follow Defendant's rationale, Plaintiff would have no recourse against the mass copyright infringement it suffers on a daily basis.

During her time as Register of Copyright, Mary Beth Peters explained the rights of copyright holders in peer-to-peer infringement actions to the Senate Judiciary Committee. "The law is unambiguous. Using peer-to-peer networks to copy or distribute copyrighted works without permission is infringement and copyright owners have every right to invoke the power of the courts to combat such activity. Every court that has addressed the issue has agreed that this activity is infringement." [1] Ms. Peters further explained that without actions like the one before this Court, infringers may never stop their conduct. "[W]hether or not these infringers know or care that it is against the law, the knowledge that such conduct may lead to expensive and burdensome litigation and a potentially large judgment should have a healthy deterrent effect." Id. She further continued that it is necessary for copyright holders to enforce the laws, because without so doing, laws without penalties will be ignored.

> While we would like to think that everyone obeys the law simply because it is the law and out of a sense of obligation, we also know that laws without penalties may be widely ignored. For many people, the best form of education about copyright in the internet world is the threat of litigation. In short, if you break the law, you should be prepared to accept the consequences. Copyright owners have every right to enforce their rights in court, whether they are taking action against providers of peer-to-peer services designed to profit from copyright infringement or against the persons engaging in individual acts of infringement using such services.

Id. (Emphasis added).

[1] Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks Statement of Marybeth Peters The Register of Copyrights before the Committee on the Judiciary 108th Cong. (2003) available at http://www.copyright.gov/docs/regstat090903.html

Defendant makes every effort to condemn Plaintiff's actions. The "pure bill of discovery" suits filed by undersigned in state courts have been approved by over a dozen judges after many hearings and briefings and are completely unrelated to this case. Undersigned's "modus operandi" is simply to protect and advocate on behalf of Plaintiff's interests. And both undersigned and Plaintiff have entered into this process eager to litigate the cases before this Court. Indeed, Plaintiff has intentionally limited the number of Defendant's in each case to facilitate litigation. Plaintiff and undersigned have served numerous individuals in these cases and will continue to do so. The scope of infringement nationwide and in this district is massive, and without bringing these suits, infringers like the putative Defendant will continue to wildly steal from Plaintiff with no fear of repercussions.

Just this past month, the Honorable Porcelli ruled on an almost identical motion filed by Defendant's counsel, finding the requested relief "inappropriate".

> The John Doe Defendants assert that the Court should limit Plaintiff's rights because this litigation is just the "tip of the proverbial iceberg" and that this type of litigation will soon become a common occurrence on the Court's docket (Dkt. No. 24 at 19-20). The John Doe Defendants request that the Court take an active role and utilize its inherent power to limit how Plaintiff may proceed in this case. Essentially, the John Doe Defendants are requesting the Court create a special exception under the Copyright Act for cases such as this in which the copyrighted material contains pornography.[3] The Court is simply not inclined to take such an inappropriate action.

Malibu Media, LLC v. John Does 1-9, 8:12-cv-669-T-23AEP, *7 (M.D. Fla. July 6, 2012) (Emphasis added).

II. JOINDER IS PROPER

"Joinder of parties is generally encouraged in the interest of judicial economy." Nu Image, Inc. v. Does 1-3,932, 2:11-CV-545-FTM-29, 2012 WL 646070 (M.D. Fla. Feb. 28, 2012) report and recommendation adopted, 2:11-CV-545-FTM-29, 2012 WL 1890632 (M.D. Fla. May 23, 2012). Joinder in BitTorrent copyright infringement cases has been thoroughly analyzed in

many opinions and has been permitted where: (a) the complaint clearly explains how BitTorrent works through a series of transactions, (b) all of the defendants live in the district (eliminating long-arm issues and venue), (c) all of the defendants were part of the same exact swarm of peer infringers as evidenced by a unique cryptographic hash value, and (d) Plaintiff pled that the Defendants' are jointly and severally liable for each others' infringement.

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

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

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

A. The Defendant's Conduct Arose Out of a Series of Transactions

Here, joinder is being asserted because the defendants interacted with each other in one of four ways.

1) the Defendant connected to and transferred a piece of the Movie **from the initial seeder;** or

2) the Defendant connected to and transferred a piece of the Movie **from a seeder** who downloaded the completed file from the initial seeder or from other peers; or

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

Patrick Collins, Inc. v. John Does 1-21, CIV.A. 11-15232, 2012 WL 1190840 at *5 (E.D. Mich. Apr. 5, 2012). Each defendant is related to each other in a logical way. The defendants are linked to each other, at minimum, through the initial seeder who first offered the torrent file. Then, because the BitTorrent protocol requires defendants to connect their computers with each other to receive pieces of the infringed movie, the defendants participated in and furthered the chain of infringement by facilitating downloading for others while receiving downloaded pieces from other defendants and infringers.

> **This relatedness arises not merely because of their common use of the BitTorrent protocol, but because each Defendant affirmatively chose to download the same Torrent file that was created by the same initial seeder**, intending to: 1) utilize other users' computers to download pieces of the same Movie, and 2) allow his or her own computer to be used in the infringement by other peers and Defendants in the same swarm.

Patrick Collins, Inc., 2012 WL 1190840 at *5. (Emphasis added).

B. The Supreme Court Allows Joinder When The Defendants Do Not Know Each Other and The Events Occurred At Different Times

The Supreme Court has ruled joinder is proper when, like this case, defendants' actions arose out of the same system of conduct, even if they did not interact directly with each other. In United States v. Mississippi, 380 U.S. 128 (1965) the Supreme Court found that the joinder of six defendants, election registrars of six different counties, was proper because the allegations were all based on the same state-wide system designed to enforce the voter registration laws in a way that would deprive African Americans of the right to vote. Although the complaint did not allege that the registrars directly interacted with each other, or even that they knew of each

other's actions, or that each other's actions directly affected each other in any way, the Supreme Court interpreted Rule 20 to hold a right to relief severally because the series of transactions were related and contained a common law and fact. Id. at 142-143.

> [T]he complaint charged that the registrars had acted and were continuing to act as part of a state-wide system designed to enforce the registration laws in a way that would inevitably deprive colored people of the right to vote solely because of their color. On such an allegation the joinder of all the registrars as defendants in a single suit is authorized by Rule 20(a) of the Federal Rules of Civil Procedure.

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

Likewise, in the case at hand, the defendants are properly joined because their actions directly relate back to the same initial seed of the swarm, and their alleged infringement further advances the series of infringements that began with that initial seed and continued through other infringers. In doing so, the defendants all acted under the same exact system. Defendants shared pieces that originated from the same exact file, and opened their computer to allow others to connect and receive these pieces.

C. Joinder Creates Judicial Litigation Economies

Joinder of the defendants creates judicial efficiency, particularly at this stage of the litigation process, and is beneficial to the Doe Defendants.

> The Court finds no prejudice to the Defendants at this stage in the litigation. In fact, the Court finds that joinder in a single case of the Defendants who allegedly infringed the same copyrighted material both promotes judicial efficiency and benefits the Defendants, who will be able to see the defenses, if any, raised by other John Does.

K-Beech, Inc. v. Does 1-57, 2:11-CV-358-FTM-36, 2011 WL 5597303 (M.D. Fla. Nov. 1, 2011). Defendant, on the one hand, claims Plaintiff has filed too many cases in this Court and this Court should derive an improper purpose from Plaintiff's actions. See Def's Mot. 3. On the other hand, Defendant argues the Court should sever and force Plaintiff to file more cases,

against each individual Defendant. See Def's Mot. 7. This argument is simply not logical. For itself and the Court, as stated above, Plaintiff intentionally limited the number of Doe Defendants in this case to a manageable number.

If this Court were to sever, at every stage of the process, the litigants and the Court would be faced with additional work. For example, instead of one motion for leave to serve subpoenas in advance of a 26(f) conference, there would be many such identical motions. Instead of one Rule 26(f) conference and report, there would be many such identical Rule 26(f) conferences and reports. Identical pleadings and papers would be repetitively filed. The Court would be required to enter the same orders multiple times. Not only would this needlessly increase the costs for the parties and Court but also for the third party internet service providers.

Defendant unconvincingly argues that the Court should sever because the formal discovery process will be unmanageable for the Court and prejudice defendants. As an initial point, a joined case in the discovery process would likely benefit the defendants who would be able to see multiple discovery requests from different counsel. But should the Court choose to revisit this issue at a later date, either by motion or *sua sponte*, the Court may do so. See Fed. R. Civ. P. 21. As the Eastern District of Pennsylvania noted, "consolidating early discovery for the purpose of determining the scope of claims and defenses will foster judicial economy." Raw Films, Ltd. v. John Does 1-15, CIV.A. 11-7248, 2012 WL 1019067 (E.D. Pa. Mar. 26, 2012).

III. THIS COURT SHOULD NOT ISSUE A PROTECTIVE ORDER

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

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

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

Id. at *4 (citing Liberty Media Holdings, LLC v. Swarm Sharing Hash File AE340D0560129AFEE8D78CE07F2394C7B5BC9C05, 821 F. Supp. 2d 444 (D. Mass. 2011). Just within the last week, this Court found that a protective order was unwarranted because Plaintiff has demonstrated good cause for the discovery. See Malibu Media v. John Does 1-13, 2:12-cv-0177-JES-SPC (M.D. Fl. June 6, 2012).

A. The Information Plaintiff Requests is Relevant

This Court granted Plaintiff limited discovery to serve a subpoena on Defendant's ISP because Plaintiff has no other way to identify the Defendants and proceed with its copyright infringement case against them. Plaintiff has requested only the identifying information of the Defendants from their ISPs. As the Honorable Judge Porcelli held, "[t]he information sought by Plaintiff falls squarely within this broad scope of discovery and is therefore warranted in this matter." Malibu Media, LLC v. John Does 1-9, 8:12-cv-669-T-23AEP, *4 (M.D. Fla. July 6, 2012).

> Clearly the identity of the ISP customer is relevant under Rule 26, in that it is "reasonably calculated" to lead to the identity of the infringer whether it is the ISP customer or some other individual. Therefore, the Court finds that any concern about identifying a potentially innocent ISP customer, who happens to fall within the Plaintiff's discovery requests upon the ISPs, is minimal and not an issue that would warrant the Court to exercise its inherent power to govern these discovery matters by minimizing or prohibiting the otherwise legitimate, relevant, and probative discovery.

Id. at *5.

> As other courts have explained, the information Plaintiff seeks is highly relevant.
>
> The Court found good cause for ordering that discovery, *see* Fed.R.Civ.P. 26(b)(1), because the plaintiff showed that a subpoena seeking the subscriber information associated with the allegedly infringing IP addresses would be the only way for the plaintiff to identify the proper defendants in this case and proceed with its claims against them.[3] *See* Declaration of Tobias Fieser ¶ 9, 23, Pl.'s Mot. Ex. The information sought is thus highly relevant to the plaintiff's claims.

Raw Films, Ltd. v. John Does 1-15, CIV.A. 11-7248, 2012 WL 1019067, at *6 (E.D. Pa. Mar. 26, 2012).

The Eastern District of Pennsylvania court also noted that Fed. R. Civ. P. 26(b)(1) permits parties to obtain discovery of "the identity and location of persons who know of any discoverable matter." Id. at *14. When addressing the issue of whether the infringer is the account holder of the IP address, the Court stated "[t]hese are not grounds on which to quash a subpoena otherwise demonstrated to be proper. The moving Doe may raise these and any other nonfrivolous defenses in the course of litigating the case." Id.

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

Defendant also relies heavily on the Eastern District of New York opinion where Judge Brown questioned the likelihood the infringer was the owner of the IP Address. See Def's Mot. at ¶ 6. Plaintiff respectfully disagrees with Magistrate Judge Brown's opinion and believes that recent technological advances make it more likely that a wireless account will be secured and can easily be traced to a household where the subscriber either is the infringer or knows the

infringer. Recently, PC Magazine published an article regarding the scarcity of open wireless signals. "These days, you are lucky to find one in 100 Wi-Fi connections that are not protected by passwords of some sort."[2] The author continues to explain why routers are now more likely to be secured. "The reason for the change is simple: the router manufacturers decided to make users employ security with the set-up software. As people upgrade to newer, faster routers, the wide-open WiFi golden era came to an end."[3] This article, published on March 26, 2012, runs contrary to Judge Brown's assertions and supports the idea that most households do have closed, protected wireless that are not likely to be used by a neighbor or interloper.

Further, Plaintiff uses the same process as Federal Law Enforcement to identify cyber crimes. In a Statement of Deputy Assistant Attorney General Jason Weinstein before the Senate Judiciary on Privacy, Technology and the Law, he discusses how Federal law enforcement use IP addresses to identify an individual.

> When a criminal uses a computer to commit crimes, law enforcement may be able, through lawful legal process, to identify the computer or subscriber account based on its IP address. This information is essential to identifying offenders, locating fugitives, thwarting cyber intrusions, protecting children from sexual exploitation and neutralizing terrorist threats.[4]

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

> The Court acknowledges that Verizon's compliance with the subpoena may not directly reveal the identity of an infringer. Indeed, the subscriber information Verizon discloses will only reveal the account holder's information, and it may be that a third party used that subscriber's IP address to commit the infringement alleged in this case.

Raw Films, Ltd. v. John Does 1-15, CIV.A. 11-7248, 2012 WL 1019067 (E.D. Pa. Mar. 26, 2012). (Internal citations omitted). The Court went on to note that while the IP address did not

[2] See Free Wi-Fi is Gone Forever www.pcmag.com/article2/0,2817,2402137,00.asp).
[3] Id.
[4] Statement of Deputy Assistant Attorney General Jason Weinstein Before the Senate Judiciary Subcommittee on Privacy, Technology and the Law available at www.justice.gov.

guarantee the subscriber was the infringer, "[t]he subpoena is specific enough to give rise to a reasonable likelihood that information facilitating service upon proper defendants will be disclosed if the ISPs comply." Id.

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

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

> A more thorough approach to detecting infringement in BitTorrent would be to adopt the stated industry practice for monitoring the Gnutella network: in the case of suspected infringement, download data directly from the suspected user and verify its contents. Because we have notified several enforcement agencies … we expect increasing use of direct downloads for verifying information.[5]

(Emphasis added.) Plaintiff used this exact process to identify Defendant's IP address. Plaintiff's investigative service, IPP Limited, established a direct one to one connection with a computer using Defendant's internet service and received a piece of Plaintiff's copyrighted movie from that computer. "A direct and continuous connection between the IPTRACKER-server and the uploader of the file is established and exists at least 10 seconds before, during and at least 10 seconds after the capture sequence i.e. during the whole download process." (Dec. Tobias Feiser Ex. A. at *4.)

Further, as Defendant's study suggests, Plaintiff has taken additional safeguards for accuracy by verifying the content received from Defendant.[6] Plaintiff has a human "in the loop" to provide a manual check of the identifying material. As Plaintiff's investigator, Tobias Fieser,

[5] Def.'s Mot. 16 citing Michael Piatek, Tadayoshi Kohno, & Arvind Krishnamurthy, *Challenges and Directions for Monitoring P2P File Sharing Networks – or – Why My Printer Received a DMCA Takedown Notice*, 3rd USENIX Workshop on Hot Topics in Security (HatSec '08), July 2008.
[6] Piatek at *6.

attests, "I analysed each BitTorrent 'piece' distributed by each IP address listed on Exhibit B and verified that reassembling the pieces using a specialized BitTorrent Client results in a fully playable digital motion picture." (Dec. Tobias Fieser at ¶ 21.) Plaintiff is absolutely certain that Defendant's IP address downloaded, controlled, and distributed Plaintiff's copyrighted work to its investigative service. Defendant's study supports Plaintiff's findings.

C. Plaintiff's Investigation Is Proper

Plaintiff legally obtained Defendant's IP address through its investigators use of the IPTRACKER software. Plaintiff's investigator did not violate Florida Statute section 493.6120(1) because it is not subject to Florida law and, moreover, Defendant failed to submit a valid argument or any authority in support of the applicability of the Florida statute to this case. Defendant contends that Plaintiff's method of obtaining an investigator from a German company to review and confirm Doe's involvement in downloading copyrighted materials is illegal. Def's Mem. 16. To support its position, Defendant cites a Florida statute that states it is a misdemeanor for an unlicensed investigator, who is not a United States citizen or permanent legal resident alien, to conduct a private investigation. Def's. Mem. 16; Fla. Stat. 493.6120(1) (2012); Fla. Stat. 493.6106(f) (2011).

In Capitol Records Inc. v. Thomas-Rasset, 680 F.Supp.2d 1045, 1058 (D. Minn. 2010) the District Court of Minnesota rejected this exact argument. Specifically, a putative peer to peer copyright infringement defendant argued that the plaintiff's private detective was guilty of a misdemeanor for failing to obtain a state private investigative license. Id. The court denied the motion by holding that "[d]efendant points to no New Jersey case or statute that holds that evidence obtained by an unlicensed private detective is subject to suppression" and "[defendant] provides no substantive legal argument or factual analysis of whether the New Jersey statute would apply at all in this case." Id.

Just as in Capitol Records Inc., Defendant fails to provide a substantive or factual argument to support his position that Florida Statute section 493.6120(1) applies to this case. Defendant also has not, and cannot, cite to any case law that illustrates the applicability of this statute to internet investigations, much less any investigation. Rather, Defendant merely draws language from the statute to emphasize the alleged failure of Plaintiff's forensic analyst to comply with licensing requirements without recognizing that the he is not subject to the statute. Def's Mem. 16. The investigator did not operate in Florida, did not conduct the investigation in Florida, or participate in any other activities relating to this case within the State of Florida. See Healy v. Beer Inst., 491 U.S. 324, 36 (1989) (a statute that seeks to control commerce occurring wholly outside the boundaries of a State "exceeds the inherent limits of the enacting State's authority and is invalid").

Further, the ABA has reported that requiring the licensure of computer forensic investigators is not practical because of the widespread use of the internet on globally connected computers. See American Bar Association, Section on Science and Technology Law, *Resolution on Computer Forensic Licenses*, p. 2 (adopted Aug. 11-12, 2008). The adopted recommendation[7] by the American Bar Association ("ABA") stated that "[a] patchwork of differing state licensing requirements for computer forensic and network testing assistance will create jurisdictional complexities that will hamper business operations and court proceedings, disadvantage litigants, and may deprive courts of hearing the best available evidence." Id. Moreover, requiring licenses may not only present jurisdictional obstacles, but it also may have a negative impact on the courts. As noted in the recommendation, "not all licensed private

[7] The recommendation, adopted in 2008, urged states to refrain from requiring computer forensic investigators to obtain licenses.

investigators are qualified to perform computer forensic services and many qualified computer forensic professionals would be excluded because they are not licensed."[8] Id.

Defendant's argument further fails because the IPTRACKER software only received information that was already publicly available to the thousands of users on the BitTorrent system. Indeed, a computer utilizing Defendant's IP Address willfully connected to the investigator's server and offered the information. Courts have held that individuals who use the internet to illegally copy and distribute copyrighted material have a minimal expectation of privacy "because those individuals have already voluntarily given up certain information by engaging in that behavior." Raw Films, Ltd. v. John Does 1-15, CIV.A. 11-7248, 2012 WL 1019067 at *8 (E.D. Pa. Mar. 26, 2012). See also In re Verizon Internet Servs., Inc., 257 F.Supp.2d 244, 267 (D.D.C.2003) (sharing files on a peer-to-peer program is "essentially opening up the computer to the world"). In this case, Defendant connected to Plaintiff's server and directly transmitted to Plaintiff a piece of Plaintiff's movie. Dec. of Tobias Feiser ¶ 18.

As Defendant correctly noted, the IPTRACKER software "use[s] hash value to search for lists of potential sources [of data] on the internet by IP address." Def's Mem. 18. This software merely collected and recorded the publically available IP addresses of internet users who illegally downloaded and distributed Plaintiff's copyrighted material. Because a file sharing program only allows users to send and receive requests for specific files, and does not permit a user to gain access of another user's computer, the IPTRACKER did not receive confidential information, but rather the public IP addresses of users exchanging files. As such, Plaintiff did not conduct a "private" investigation because the IP address it received was publicly distributed on the BitTorrent software.

[8] The ABA also recognized another important distinction between private and computer forensic investigators by stating that "[p]rivate investigation licenses are not adequate determinants of competency in a field driven by technological innovation and science" and "expert testimony in computer forensics should be based upon the current state of science and technology . . . and the education of the expert." Id.

Defendant's conclusion that the process Plaintiff uses to identify Defendant's IP Address is improper is without basis. It is necessary for Plaintiff to download a part of its movie to determine that Defendant is in fact distributing it. It is not copyright infringement when Plaintiff downloads because Plaintiff owns the copyright. Plaintiff makes clear it does not upload the movie, or further distribute it to any other peers in the swarm. See Dec. of Tobias Feiser Ex. A. As stated above, Plaintiff utilizes the most reliable and reasonable efforts to verify the infringement.

III. CONCLUSION

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

Dated: September 13, 2012

Respectfully submitted,

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

CERTIFICATE OF SERVICE

I hereby certify that on September 13, 2012, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF and that service was perfected on all counsel of record and interested parties through this system.

By: /s/ *M. Keith Lipscomb*