UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

MALIBU MEDIA, LLC, Plaintiff, v. JOHN DOE subscriber assigned IP address 99.169.76.167, Defendant.	)	Civil Action Case No. 1:13-cv-23714-UU

PLAINTIFF'S RESPONSE TO THE COURT'S ORDER TO SHOW CAUSE [CM/ECF 6]

I. INTRODUCTION

Statistics demonstrate that the Internet Protocol Address ("IP Address") geolocation tracing process used by Plaintiff here, accurately predicted in counsel's prior cases that a Doe defendant's IP Address would trace to the state of Florida and the Southern District of Florida 100% of the time. The score is 83 out of 83. Eleventh Circuit law requires that a Court construe all reasonable inferences in favor of Plaintiff and that Plaintiff need only demonstrate a *prima facie* case of personal jurisdiction and venue. Here, Plaintiff has established a *prima facie* case of personal jurisdiction and venue because its geolocation database has correctly provided traces to this state and district 100% of the time. And, Plaintiff uses the same procedures as law enforcement.

Plaintiff's investigator, IPP International UG, utilizes technology which ensures that a defendant's IP address is correctly recorded at the exact time of infringement and is always accurate. The Defendant in this case repeatedly infringed twenty of Plaintiff's copyrighted works over the course of six months. Without being able to establish jurisdiction based on geolocation technology, Plaintiff cannot enforce its right to sue online infringers. There is simply no other way. For these reasons, as more fully explained below, Plaintiff respectfully requests that this Honorable Court find that Plaintiff has satisfied its burden of pleading that Florida has personal jurisdiction over Defendant and that the Southern District of Florida is the proper venue.

II. FACTS

A. Plaintiff's Use of Geolocation Technology Has Resulted In 100% Accuracy in this District

IPP International UG ("IPP") provided Plaintiff with the Doe Defendants' IP addresses, hit dates of infringement and the correlating hash values for each infringement. *See* Declaration of Tobias Fieser, Exhibit A. Thereafter, each IP Address present within the abovementioned forensic data is automatically referenced against Maxmind® Premium's IP geolocation database[1]. Plaintiff then, when forming its suit, verifies that each Doe Defendant was using an IP Address assigned to a location inside the Southern District of Florida. Plaintiff only forms its suits against defendants that have reputable Internet Service Providers ("ISPs"), such as here, AT&T,

[1] As an example of how the process works, www.maxmind.com/en/geoip_demo provides a way for anyone to test the database which Plaintiff uses. Here, Plaintiff inputted Defendant's IP address and received the same information it originally received from Maxmind. *See* Exhibit B.

which from Plaintiff's experience have consistently traced to the city location provided by Maxmind.

Statistics from undersigned's prior cases in this district using Maxmind geolocation technology demonstrate that this process accurately predicted that a Doe defendant's IP Address would trace to the Southern District of Florida 100% of the time. The score is 83 out of 83. *See* Declaration of Emilie Kennedy and Jason Cooper, Exhibit C.

B. IPP's Technology Records the Exact Date and Time of the Infringement

Michael Patzer is the creator of the software which IPP uses to detect infringement. *See* Declaration of Michael Patzer at ¶ 3, Exhibit D. Mr. Patzer also testified at the Bellwether trial in Philadelphia.[2] *See Malibu Media, LLC v. John Does 1, 6, 13, 14,* 12-cv-02078, (E.D. Pa. June 10, 2013) at CM/ECF 195-196].

The IP detection process begins when IPP's clients, here Malibu Media, provide IPP with the names of their copyrighted works. *Id*. at ¶ 7. IPP's software then scans the index of torrent websites for possible matches using a lexical search. *Id*. at ¶ 8. If IPP's servers find a possible match, the computer file associated with the .torrent file is downloaded and the logging process begins. *Id*. at ¶ 9. After a possible match is found through a lexical search, IPP immediately starts downloading the computer file associated with the .torrent file, and logging transactions. *Id*. at ¶ 13. "Logging transactions" means that IPP's servers start requesting data from the possible infringers, and storing that information on a database server. *Id*. at ¶ 14.

IPP saves the transactions on a WORM tape drive. "WORM" stands for write-once-read-many, which means that one can only write to the tape drive once, but the tape drive can be read many times. In this manner, modification of what is written onto the WORM tape drive is impossible. *Id*. at ¶ 15. The transactions are saved in a type of computer file known as a PCAP file. "PCAP" stands for Packet Capture, and the type of "packet" being captured is a data packet. *Id*. at ¶ 16. IPP uses a program called TCP-Dump to create PCAPs. TCP-Dump records all of the network transactions that a server receives and transmits. *Id*. at ¶ 17. In this manner, TCP-Dump works like a video camera recording all of the ins-and-outs of transactions to and from IPP's servers. *Id*. at ¶ 18. IPP also saves the downloaded computer files which correlate to the .torrent files onto the WORM tape drive. *Id*. at ¶ 19. The WORM tape drives receive a time

[2] On June 10, 2013, Malibu Media became the first Plaintiff to ever try a BitTorrent copyright infringement case. *Id.* at ¶ 33. The "Bellwether" case ended with final judgments in Plaintiff's favor against all three defendants. *Id.* at ¶ 34.

stamp issued by the German government. This time stamp is recorded on the WORM tape drive within twenty-four hours after a PCAP file is placed on the drive. *Id*. at ¶ 20. This time stamp proves that the data was actually written at that time. *Id*. at ¶ 21. IPP uses approximately 150 servers and two tape robots. *Id*. at ¶ 22. In terms of security certifications, IPP fulfills the security standard used by companies for processing credit card data. *Id*. at ¶ 23.

It is important that IPP's servers have the correct time because ISPs use that data to correlate the alleged infringement to a subscriber. *Id*. at ¶ 24. The clocks for IPP's servers are set using GPS time, as set by two dedicated GPS servers and by an atomic clock. *Id*. at ¶ 25. If the time for IPP's servers is different from either the GPS time or the atomic time by any more than one hundredth (0.01) of one second, IPP does not log the transaction. *Id*. at ¶ 26. The specific length of time IPP's system is set up to maintain a connection during each transaction with an alleged infringer is two seconds before and two seconds after data is transferred. *Id*. at ¶ 27.

Accordingly, since the time for IPP's servers is never inaccurate by more than a hundredth (0.01) of one second, and IPP maintains connections for more than four seconds, the ISPs are able to accurately correlate the detected infringement to a particular subscriber. *Id*. at ¶ 28. After IPP's WORM tape drives are filled with data, they are stored in a data security safe. *Id*. at ¶ 29.

C. Before Signing Each Declaration, IPP Double Checks That the IP Address Is the Same IP Address It Recorded Infringing to Ensure Accuracy

Before this suit was created, IPP sent Malibu Media's counsel infringement data. *Id*. at ¶ 21. After receiving the geolocation information from Maxmind, Malibu Media's counsel then sends to Tobias Fieser a proposed declaration in support of this suit and with attached exhibits from the Complaint. *Id*. at ¶ 22. Mr. Fieser then verifies that the information contained on these exhibits was accurate by taking the Microsoft Word documents sent by Malibu Media's counsel and cutting and pasting the information in them into a Microsoft Excel document, which he then uploads into IPP's computer system. *Id*. at ¶ 23. If all of the information is correct in the Microsoft Word document, IPP's program displays a green light on his computer screen, which occurred in this case with respect to Exhibit A of the Complaint. *Id*. at ¶ 24. This ensures that no errors were made with the IP address from the time IPP sent Plaintiff the information until the time when the Complaint and Motion for Leave are filed.

D. Plaintiff Has Hired an Expert to Individually Test IPP's Technology

Plaintiff knows IPP's technology works with 100% certainty because it hired a third party computer investigations expert, Patrick Paige, to independently test IPP's IP Address detection method. *See* Declaration of Patrick Paige ("Paige Decl."), Exhibit E. Patrick Paige was a detective in the Palm Beach County Sherriff's computer crimes unit. *Id*. at ¶ 2. His results concluded that it works. *Id*. at

E. Defendant's Continuous Infringement Ensures That Identifying Him is Likely

Plaintiff only sues habitual and persistent infringers of its movies. Here, IPP recorded the IP address assigned to Defendant illegally infringing twenty (20) different movies owned by Plaintiff from February 5, 2013 to August 16, 2013. *See* Complaint, Exhibit A [CM/ECF 1-2]. The infringement occurred for more than a six month period from this IP address demonstrating that the infringer had consistent and continuous access to the IP address.

III. LEGAL ARGUMENT

A. Plaintiff Has Established a Prima Facie Case of Personal Jurisdiction

Plaintiff properly pled that this Court has personal jurisdiction over Defendant. *See* Complaint at ¶ 5. "The district court must construe the allegations in the complaint as true, to the extent they are uncontroverted by defendant's affidavits or deposition testimony." *Morris v. SSE, Inc.*, 843 F.2d 489, 492 (11th Cir. 1988) (analyzing dismissal in a personal jurisdiction context). "Where there is conflicting evidence, the court must construe all reasonable inferences in favor of the plaintiff." *Structural Panels, Inc. v. Texas Aluminum Indus., Inc.*, 814 F. Supp. 1058, 1063 (M.D. Fla. 1993) citing *Cable/Home Commc'n Corp. v. Network Prods., Inc.*, 902 F.2d 829, 855 (11th Cir. 1990). "[A] motion to dismiss at the pleading stage for lack of personal jurisdiction should also be treated with caution, and denied if the plaintiff alleges sufficient facts in his complaint to support a reasonable inference that the defendant can be subjected to jurisdiction within the state." *Bracewell v. Nicholson Air Servs., Inc.*, 680 F.2d 103, 104 (11th Cir. 1982).

Under Florida's personal jurisdiction statute a defendant "submits himself or herself ... to the jurisdiction of the courts of this state for any cause of action arising from the doing of any of the following acts: 1. Operating, conducting, engaging in, or carrying on a business or business venture in this state or having an office or agency in this state; 2. Committing a tortious act within this state." Fla. Stat. § 48.193.

"The plaintiff must establish a prima facie case of personal jurisdiction." *Cable/Home Commc'n Corp. v. Network Prods., Inc.*, 902 F.2d 829, 855 (11th Cir. 1990). "A prima facie case ... consists of sufficient evidence ... to get plaintiff past a motion for directed verdict in a jury case or motion to dismiss in a nonjury case. It is the evidence necessary to require the defendant to proceed with his case." *Bracewell v. Nicholson Air Servs., Inc.*, 748 F.2d 1499, 1504 (11th Cir. 1984).

Here, construing all the facts in the light most favorable to Plaintiff, it is reasonable for the Court to find that this Court has personal jurisdiction over Defendant. Plaintiff has alleged that Defendant has committed a tort in this state by infringing Plaintiff's copyrights twenty times. Maxmind geolocation technology, which traced Defendant to a location in Miami, FL, has always been 100% accurate when traced to the Southern District of Florida, and has been tested 83 separate times. Although there does exist a remote possibility that Maxmind incorrectly traced Defendant's IP address to the state of Florida, it is reasonable to assume that it traced correctly because it always has done so before. "These allegations are sufficient to allege personal jurisdiction in this case." *See Malibu Media, LLC v. John Does 1-25*, 2:12-CV-266-FTM-29, 2012 WL 3940142 (M.D. Fla. Aug. 21, 2012) (finding personal jurisdiction proper under near identical circumstances).

B. Plaintiff Has Established a Prima Facie Case of Venue

Just as Plaintiff properly pled personal jurisdiction, Plaintiff properly pled venue. *See* Complaint at ¶ 7. "A civil suit to enforce the Copyright Act may be brought in any district 'in which the defendant or his agent resides or may be found.'" *Palmer v. Braun*, 376 F.3d 1254, 1259 (11th Cir. 2004) (citing 28 U.S.C. §1400(a)). "A defendant 'may be found' in a district in which he could be served with process; that is, in a district which may assert personal jurisdiction over the defendant." *Id.*

"The facts as alleged in the complaint are taken as true, to the extent they are uncontroverted by defendants' affidavits." *Delong Equip. Co. v. Washington Mills Abrasive Co.,* 840 F.2d 843, 845 (11th Cir. 1988). "[T]he plaintiff must present only a prima facie showing of venue." *Delong Equip. Co. v. Washington Mills Abrasive Co.*, 840 F.2d 843, 845 (11th Cir. 1988). "[T]he court is inclined to give greater weight to the plaintiff's version of the jurisdictional facts and to construe such facts in the light most favorable to the plaintiff." *Home Ins. Co. v. Thomas Indus., Inc.*, 896 F.2d 1352, 1355 (11th Cir. 1990). "When venue would be

proper in another district under § 1391, transfer is preferred over dismissal unless there is evidence that a case was brought in an improper venue in bad faith or in an effort to harass a defendant." *Palmer v. Dau*, 2010 WL 2740075 (M.D. Fla. 2010) at *2 (emphasis added) (citing Wright, Miller & Kane, *Fed. Practice & Procedure: Jurisdiction 2d* § 3827 at 262 (1998 & 2005 Supp.))

Here, construing all the facts in the light most favorable to Plaintiff, it is reasonable to infer that venue is proper in the Southern District of Florida because Plaintiff's Maxmind geolocation technology which traced Defendant to a location in Miami, FL has always been 100% accurate when traced to the Southern District of Florida. The proof that the technology works is that it has always worked previously. This Court should not dismiss Plaintiff's Complaint for improper venue when there is no evidence that venue is not proper. Indeed, Defendant has not even appeared in this case.

In the event the Court is still not convinced that Plaintiff has properly established venue, Plaintiff respectfully requests the Court allow it to subpoena the ISP with the subpoena response being returnable to your Honor's chambers. If the Defendant's address is insufficient to establish venue then Plaintiff's suit will be dismissed. Alternatively, the Court could enter an order requiring Plaintiff to dismiss its suit and destroy the subpoena response if Defendant does not reside in the Southern District of Florida.

C. The Southern District of Florida is Likely to Have a Higher Rate of Geolocation Accuracy Than Other Jurisdictions

"Plaintiff can establish such a good faith basis for residence or personal jurisdiction by utilizing geolocation services that are generally available to the public to derive the approximate location of the IP addresses identified for each putative defendant." *Nu Image, Inc. v. Does 1-23,322*, 799 F. Supp. 2d 34, 40 (D.D.C. 2011). "Even when not accurate, though, geolocation can place users in a bordering city, which may be good enough for the entity seeking the information. This happens because a common method for geolocating a device is referencing its IP address against similar IP addresses with already known locations." *Id.* at 40-41.

Here, in the Southern District of Florida, Plaintiff is more likely to have accurate traces from its geolocation database because the South Florida does not border any other states. Therefore, there are no close calls where a city may fall on a border and ultimately trace to a neighboring state.

Likewise, when analyzing venue, Plaintiff's geolocation software will also be almost always accurate in this District because the Southern District of Florida Miami Division only borders the Middle District of Florida at a point where population is sparse. At worst, the geolocation software may trace to Fort Lauderdale or the Florida Keys. There is very little risk it will trace to the Middle District of Florida because of the low population in the Everglades. This likely explains why counsel's traces to the Southern District of Florida are 100% accurate.

D. Courts Consistently Find That Geolocation Technology Establishes a Prima Facia Case of Personal Jurisdiction and Venue

To undersigned's knowledge, no court has ever dismissed a complaint in a copyright infringement action for pleading personal jurisdiction or venue based on geolocation technology. Indeed, numerous courts throughout the country have consistently held that a plaintiff's use of geolocation technology is sufficient to establish a prima facie case of personal jurisdiction and venue.

"In situations where a plaintiff files suit against then unnamed defendants, courts have accepted IP addresses as establishing a prima facie case of personal jurisdiction." *Canal St. Films v. Does 1-22*, 1:13-CV-0999, 2013 WL 1775063 (M.D. Pa. Apr. 25, 2013); *see also W. Coast Prods., Inc. v. Does, 1-1911*, CV 11-1687(ABJ), 2011 WL 11049265 (D.D.C. Oct. 25, 2011) ("plaintiff could demonstrate a good faith basis for its venue allegations if a geolocation service placed the IP address in question within the District of Columbia, or within a city located within 30 miles of the District of Columbia"); *Malibu Media, LLC v. John Does 1-25*, 2:12-CV-266-FTM-29, 2012 WL 3940142 (M.D. Fla. Aug. 21, 2012) (Plaintiff sufficiently alleged personal jurisdiction by using geolocation software to trace defendants to a location in the Middle District of Florida); *Digital Sins, Inc. v. John Does 1-245*, 11 CIV. 8170 CM, 2012 WL 1744838 (S.D.N.Y. May 15, 2012) (geolocation is sufficient to allege personal jurisdiction and venue); *Digital Sin, Inc. v. Does 1-27*, 12 CIV. 3873 JMF, 2012 WL 2036035 (S.D.N.Y. June 6, 2012) (same); *John Wiley & Sons, Inc. v. Does Nos. 1-27*, 11 CIV. 7627 WHP, 2012 WL 364048 (S.D.N.Y. Feb. 3, 2012) (same); *Malibu Media, LLC v. John Does 1-15*, CIV.A. 12-2077, 2012 WL 3089383 (E.D. Pa. July 30, 2012) (geolocation establishes *prima facie* case of personal jurisdiction); *Malibu Media, LLC v. John Does 1 through 11*, 2012 WL 2921227 (S.D. Cal. July 17, 2012) (finding use of geolocation proper for the court to establish personal jurisdiction and venue over the defendant).

E. Federal Law Enforcement Consistently Rely on Geolocation Technology, Including Maxmind

Federal Law Enforcement rely on geolocation technology to identify perpetrators of online crimes. *See United States v. Cray*, 450 F. App'x 923, 932 (11th Cir. 2012) *cert. denied*, 133 S. Ct. 265, 184 L. Ed. 2d 45 (U.S. 2012) (holding that allowing testimony on IP address geolocation databases into evidence was not an error). Indeed, in some cases Federal Law Enforcement is cited as using Maxmind, the exact same database used by Plaintiff. *See United States v. Tillotson*, 2:08-CR-33, 2008 WL 5140773 (E.D. Tenn. Dec. 2, 2008) (noting that Maxmind's database correctly identified the Defendant and is sufficient to establish probable cause); *United States v. Richardson*, 4:11CR3116, 2012 WL 10382 (D. Neb. Jan. 3, 2012) (used by Homeland Security to identify the defendant).

F. Plaintiff Has Used Due Diligence and Due Care

1. IPP's Technology Ensures that the Exact Date and Time of Infringement is Reported to Ensure Data is Accurate for Dynamic IP Addresses

A dynamic IP address is one that changes periodically, as opposed to a static IP address which remains constant. At no time, however, are any two people assigned the same IP address. Internet Service Providers, such as AT&T, record which individual is in possession of an IP address at a particular time.

As set forth above and in the Patzer declaration, Exhibit D, IPP is extremely cautious to ensure that each infringement transaction is recorded at the *exact* moment it occurred. IPP's due diligence and care in recording and time stamping the transaction enables Plaintiff to provide the Defendant's ISP with the exact date and time of the infringement. The ISP then looks up who was assigned that IP address at that exact time and informs Plaintiff. If the ISP's records are inconclusive for any reason, the ISP will so inform Plaintiff and Plaintiff will dismiss its case. "Malibu [] expended[s] considerable effort and expense to determine the IP addresses of the infringing parties, and the technology employed by its consultants . . . [i]s valid." *Malibu Media, LLC v. John Does 1, 6, 13, 14*, 2013 WL 3038025, at *2 (E.D. Pa. 2013).

2. IPP Double Checks the IP Address is Correct Before Plaintiff Files Suit

To ensure there are no errors between the time when IPP logs the IP address and Plaintiff files suit, after all pleadings are made, but before Mr. Fieser signs a declaration attesting to the Defendant's infringement, Mr. Fieser uploads the information back into IPP's system and waits for a match. *See* Fieser Declaration, Exhibit A.

3. *Defendant's IP address is Not Likely to be a Coffee Shop or Open Wi-Fi Business*

Plaintiff has taken specific measures to ensure that the infringer is not likely to be an individual utilizing a coffee shop's wireless network, or any other business that provides free Wi-Fi access, by only suing infringers whose IP address has been used over a long period of time to infringe Plaintiff's works. In doing so, Plaintiff not only ensures that it sues the worst infringers, but also that it is suing an infringer that had repeated and continuous access to the IP address in the suit.

Attached as Exhibit F is the full hit data recorded by IPP for Defendant's IP address. This data represents each time that IPP recorded Defendant's IP address infringing Plaintiff's movies. Noteworthy, the dates and times (identified in UTC) indicate that it was likely someone accessing a home or residential internet service. As an example, on February 12, 2013 from between 1:37 a.m. UTC until 9:33 a.m. UTC, IPP recorded Defendant infringing at least once every hour. This translates to from February 11, 2013 at 8:37 p.m EST until 4:33 a.m. EST.[3] It is unlikely that a coffee shop or other business would be open that late. Even if that were the case, given the overwhelming amount of times that the infringement occurred using this IP address, the coffee shop may be able to identify which individual used their Internet to infringe.

4. *The Remote Possibility of Spoofing Should Not Prevent Plaintiff From Receiving Defendant's Identity*

IPP, Limited ("IPP") established a TCP/IP connection with a computer (the "Infringer's Computer") using Defendant's IP address. *See* Declaration of Tobias Feiser at ¶ 14, Exhibit A. The Infringer's Computer sent IPP pieces of computer files that correlate (as evidenced by identical cryptographic hash values) to copies of the works covered by the Copyrights-in-Suit. *Id*. at ¶ 15. Courts consistently rule that IP geolocation technology is sufficient to receive the identity of a defendant despite the remote likelihood that spoofing may occur.[4] *See e.g. United States v. Massey*, 4:09CR506-DJS, 2009 WL 3762322 (E.D. Mo. Nov. 10, 2009) ("there

[3] http://www.timeanddate.com/worldclock/converter.html was used to convert the time from UTC to EST.

[4] Undersigned is unaware of any lawsuits wherein a defendant established that his IP address was spoofed. See e.g. *United States v. Vosburgh*, 602 F.3d 512, 525 (3d Cir. 2010) (finding the defendant could not establish any evidence that his defense that his IP address was spoofed actually occurred).

remained a likelihood or fair probability that the transmission emanated from the subscriber's premises"). This is particularly true in this case when IPP established a direct connection.[5]

Further, Plaintiff pled that Defendant, the subscriber of the IP address 99.169.76.167, is the infringer. *See* Complaint ¶ 9-10. This allegation is plausible because the person who pays for Internet services is the most likely person to use it, particularly in this circumstance where the infringement spanned over six months. *See Malibu Media, LLC v. Pelizzo*, 12-22768-CIV, 2012 WL 6680387, *3 (S.D. Fla. Dec. 21, 2012); *see also* Paige Declaration, Exhibit E. In the approximately 200 instances where former Detective Paige supervised or directly performed the investigation of a criminal matter involving a computer and the Internet, he never encountered an incident where the geolocation software did not trace to the alleged state or district. *Id*., at ¶ 21-22. And, after executing the search warrants based upon the ISPs' correlations, in all but one instance, the police officers found the evidence.[6] *Id.*, at ¶ 21. And, in all of those instances he never once encountered a situation where an individual's Internet was hacked. *Id*. at 23.

Although there is a remote chance that Defendant's Internet has been stolen, hacked or spoofed, Plaintiff has alleged that Defendant in the infringer and Defendant's IP address traced to this district. Defendant may allege "spoofing" as a defense, but Plaintiff will still have alleged proper personal jurisdiction and venue in this Court.

5. The IP Address is Not Likely Being Used as a VPN or Proxy Server

Defendant's IP address is not likely being used as a proxy server or virtual private network, ("VPN"), because Defendant would be exposing himself to contributory infringement or other liability by offering such a service through his private AT&T U-Verse Internet subscription.[7] Indeed, most proxy servers or VPNs are hosted from foreign locations in order to avoid being readily identifiable through a subpoena by an ISP.[8] As an example, the top rated VPN on "bestvpnforyou.com" is VPN4ALL which the review claims: "VPN4All servers are

---

[5] See 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 (finding that the most accurate detection methods are when an investigator establishes a TCP/IP connection).

[6] In that one instance, a next door neighbor was using the subscriber's open WiFi.

[7] Defendant would also be violating the AT&T Terms of Service. See http://www.att.com/u-verse/att-terms-of-service.jsp ("AT&T U-verse Services are provided for your non-commercial personal use only, and for your enjoyment in a single private residential dwelling unit. You agree not to reproduce, duplicate, copy, sell, transfer, trade, resell or exploit for any commercial purposes any portion of the Services, use of the Services, or access to the Services.")

[8] http://www.bestvpnforyou.com/vpn-reviews/

located in a jurisdiction where Internet logs, personal information, account data and all client information is not required to be logged." *Id*. Other reviews of VPNs have similar descriptions.

G. Plaintiff Recently Prevailed at Trial, Courts Have Held Plaintiff is Likely to Prevail Again

On June 10, 2013, Malibu Media became the first plaintiff to ever try a BitTorrent copyright infringement case. *Id.* at ¶ 10. The "Bellwether" trial was presided over by the Honorable Michael M. Baylson, United States District Court Judge for the Eastern District of Pennsylvania. *Id.* at ¶ 11. The Bellwether case ended with final judgments on liability in favor of Plaintiff against all three defendants who were tried. *Id.* at ¶ 12. And, a final judgment on damages was entered in an amount of $112,500 plus attorneys' fees and costs against defendant Bryan White. *Id.* "The evidence that Malibu presented at trial was persuasive as to the fact that it had suffered real damages as a result of illegal downloading of its movies through BitTorrent." *Malibu Media, LLC v. John Does 1, 6, 13, 14*, 2013 WL 3038025, *8 (E.D. Pa. June 18, 2013).

Likewise, numerous courts have identified Plaintiff as having a "likelihood of success on the merits". *See Malibu Media, LLC v. Etter*, 1:12-CV-01115-TWP, 2013 WL 5366355 (S.D. Ind. Sept. 24, 2013). And, Plaintiff's Complaint has recently survived summary judgment in this District. *See Malibu Media, LLC v. Fitzpatrick*, 1:12-CV-22767, 2013 WL 5674711 (S.D. Fla. Oct. 17, 2013).

H. Copyright Owners Must Have a Process To Sue Online Infringers

Congress enacted the Digital Theft Deterrence Act of 1999 to deter online infringement by increasing the penalties therefore. *See Sony v. Tennenbaum*, 660 F.3d 487, 497 (1st Cir. 2011) (citing the Congressional record and holding that non-commercial individuals commit infringement by distributing copyrighted works online). The Supreme Court held that the sharing of copyrighted works on-line is infringement; *see Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd*. 545 U.S. 913, 125 S.Ct. 2764 (2005); so too has the Ninth Circuit *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1013 (2001). Two circuit courts opined that Rule 45 subpoenas may be used to identify online copyright infringers. *See In re Charter Communications, Inc. Subpoena Enforcement Matter*, 393 F.3d 771, 774 (8th Cir. 2005); *Arista Records, LLC. v. Doe 3*, 604 F.3d 110 (2d Cir. 2010). The Register of Copyrights testified

before Congress that adult entertainment companies have the right to sue for peer-to-peer infringement and they should not apologize for doing so.[9]

The only way to enforce one's copyrights against online infringement is to subpoena the identity of the subscriber whose internet was used to commit the infringement. And, in order to do so, a copyright holder must file a federal lawsuit and establish personal jurisdiction and venue by utilizing geolocation technology. Without this ability, copyright owners would have a right without a remedy. Any such state of affairs would violate Chief Justice Marshall's often cited rule that "the very essence of civil liberty certainly consists in the right of every individual to claim the protection of the laws, whenever he received an injury." *Marbury v. Madison*, 1 Cranch 137, 1803 WL 893, *17 (U.S. 1803). Chief Justice Marshall continued "[t]he government of the United States has been emphatically termed a government of laws, and not of men. It will certainly cease to deserve this high appellation, if the laws furnish no remedy for the violation of a vested legal right." *Id.* The U.S. still deserves that high appellation because it steadfastly creates remedies when vested rights have been infringed. The case in front of the bar is no exception, our government and laws provide copyright owners with the ability to ascertain the identity of infringers through a Rule 45 subpoena when, as here, there is a reasonably likelihood that Defendant resides in this district.

IV. CONCLUSION

For the foregoing reasons, this Court should not dismiss the case for improper venue or personal jurisdiction.

[9] "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 …While copyright owners have expressed regret that they have felt compelled to take this step, they need offer no apologies." 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

Respectfully submitted,

By: /s/ *M. Keith Lipscomb*

M. Keith Lipscomb (429554)
klipscomb@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 November 12, 2013, 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*