

JH

FILED

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS**

DEC 27 2012
DEC 27, 2012
THOMAS G. BRUTON
CLERK, U.S. DISTRICT COURT

MALIBU MEDIA, LLC,

Plaintiff,

Case No. 1:12-cv-07579
Honorable Edmond E. Chang

v.

John Does 1-23,

Defendant.

**DEFENDANT'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT FOR FAILURE
TO STATE A CLAIM UPON WHICH RELIEF MAY BE GRANTED**

I, Defendant John Doe # 16 ("Defendant"), hereby moves to dismiss Malibu Media, LLC's ("Plaintiff's") Complaint for failing to state a claim upon which relief may be granted. In support thereof, Defendant states as follows:

INTRODUCTION

Plaintiff's Complaint alleges that Plaintiff's materials were reproduced and distributed through a series of BitTorrent transactions conducted using a computer accessing the internet and identified through an Internet Protocol ("IP") address assigned to the Defendant's internet account. The entirety of these claims hinge upon Plaintiff's purely speculative conclusion that "The ISP to which each Defendant subscribes can correlate the Defendant's IP address to the Defendant's true identity." (Complaint ¶19) This conclusion is prefaced exclusively on the review of a company called IPP, Limited. There is no information whatsoever as to who this company is or what expertise they may have or details how the Plaintiff concluded that Defendant actually committed any volitional act of copyright infringement as required to sustain a claim of direct copyright infringement. In fact, the limited information provided to support Plaintiff's already thread-bare claims, as will be discussed below, is factually inaccurate and misleading. The Plaintiff's Complaint does not provide any allegation that Defendant violated any of Plaintiff's rights apart from this conclusory statement and should be dismissed. See, e.g., Cory v. Allstate

Ins., 583 F.3d 1240, 1244 (10th Cir. 2009)("[C]onclusory allegations without supporting factual averments are insufficient to state a claim on which relief can be based.")).¹

I. LEGAL STANDARD

To survive a motion to dismiss for failure to state a claim, a complaint must satisfy the pleading requirements set forth in Federal Rule of Civil Procedure 8(a)(2). While Rule 8's pleading standard "does not require 'detailed factual allegations,' . . . it demands more than an unadorned, the-defendant-unlawfully-harmed-me accusation." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)(citing *Bell Atl. Corp., v. Twombly*, 550 U.S. 544, 555 (2007)). Consequently, to survive a motion for dismissal, a "complaint's allegations must plausibly suggest that the plaintiff has a right to relief [and raise] the possibility above a 'speculative level'." *Effkay Enters. v. J.H. Cleaners, Inc.*, 2008 U.S. Dist. LEXIS 46127 at *4-5 (D. Colo. June 5, 2008)(citing *Twombly*, 127 U.S. at 1964-65)). The court is to "assume the factual allegations are true and ask whether it is plausible that the plaintiff is entitled to relief." *Gallagher v. Shelton*, 587 F.3d 1063, 1068 (10th Cir. 2009), however the "tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions. Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements do not suffice." *Iqbal*, 556 U.S. at 647. "Nor does a complaint suffice if it tenders 'naked assertions' devoid of 'further factual enhancement.'" *Khalik v. United Air Lines*, 2010 U.S. Dist. LEXIS 129598 at *4 (D. Colo. Dec. 7, 2010)(quoting *Twombly*, 550 U.S. at 557)). This "plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted

While any motion to dismiss is premised on the allegations and evidence offered by the non-moving party, Defendant believes that these actions demonstrate that Plaintiff is well aware that its allegations are routinely being made against innocent individuals who were merely internet subscribers and as a matter of policy seeks to remain willfully ignorant of this fatal defect in its pleadings.

¹ Plaintiff has already been directly warned by one Court that similar litigation behavior was inappropriate, abusive and unfair. *In re BitTorrent Adult Film Copyright Infringement Cases*, 2012 U.S. Dist. LEXIS 61447 at *19 (E.D.N.Y. 2012) . (noting that "plaintiffs have employed abusive litigation tactics to extract settlements from John Doe defendants"). Indeed, the Court went so far as to describe Plaintiff's justifications for such tactics as "rambling" and "farcical." *Id.* at n7.

unlawfully." *Patterson v. Dex Media, Inc.*, 2012 U.S. Dist. LEXIS 124067 at *4-5 (D. Colo. Aug. 31, 2012)(citing *Twombly*, 550 U.S. at 556)).

ARGUMENT

II. PLAINTIFF'S COMPLAINT SHOULD BE DISMISSED PURSUANT TO FRCP 12(b)(6) BECAUSE IT FAILS TO STATE A CLAIM UPON WHICH RELIEF MAY BE GRANTED

Dismissal of this action is warranted as Plaintiff has failed to plead any factual content allowing "the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 556)). In order to set forth a *prima facie* claim of direct copyright infringement Plaintiff must show ownership of a valid copyright² and actual violation by the defendant of one or more exclusive rights set forth in 17 U.S.C. § 106. See *Feist Pubs., Inc., v. Rural Tel. Serv. Co., Inc.*, 499 U.S. 340, 361 (1991). Pursuant to Fed.R.Civ.P. 8(a)(2), Plaintiff must plead facts sufficient to allow the Court to draw the inference that the defendant is liable for the alleged misconduct; in this case direct copyright infringement. However, Plaintiff's Complaint consists of a series of conclusory statements arranged to support the already speculative conclusion that the person paying the internet bill, the Defendant is the infringer.

A. PLAINTIFF HAS NOT PLED SUFFICIENT FACTS TO ALLOW THE COURT TO DRAW THE REASONABLE INFERENCE THAT THE DEFENDANT IS LIABLE FOR DIRECT COPYRIGHT INFRINGEMENT

Plaintiff's speculation that Defendant is the infringer is a guess. It is not supported by facts as required by Rule 8(a)(2). The sole allegation relied upon by Plaintiff in identifying the Defendant as the allegedly infringing party is that he/she was identified by their Internet Service Provider ("ISP") as the subscriber for internet service that was allegedly assigned an IP address from which Plaintiff's agent allegedly received a piece of Plaintiff's allegedly copyrighted works via the Bittorrent protocol. As a factual matter, any customer of an ISP -- such as the moving Defendant -- who connects their computer to the internet via the ISP is assigned an Internet Protocol (IP) address. In addition to the customer's IP address, the ISP's network is also assigned its own IP address. See generally *LVRC Holdings v. Brekka*, 581 F.3rd 1127, 1130 (9th Cir. 2009). An "IP address is

a series of numbers associated with a server or website, and it is used to route traffic to the proper destination on the Internet.” *Kirch v. Embarq Mgmt. Co.*, 2011 U.S. Dist. LEXIS 92701 *10 (D. Kan. Aug. 19, 2011). More specifically, an IP address identifies only the location at which one of any number of computer devices may be deployed, especially when used with a wireless router as in the instant action. As a result, one court noted that, “[b]ecause it is common today for people to use routers to share one internet connection between multiple computers, the subscriber associated with the IP address may not necessarily be the alleged infringer” *Bubble Gum Productions, LLC v. Does 1-80*, 2012 WL 2953309 at *4 (S.D.Fla. Jul. 19, 2012).

More on point, the United States District Court for the Eastern District of New York has already addressed -- in an identical case involving the current Plaintiff, Malibu Media, LLC, and its counsel Mr. Kotzker -- the erroneous assumption that an internet subscriber identified only by an IP address assigned to their account is an infringer holding that:

[T]he assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time. An IP address provides only the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones . . . Thus, it is no more likely that the subscriber to an IP address carried out a particular computer function — here the purported illegal downloading of a single pornographic film — than to say an individual who pays the telephone bill made a specific telephone call.

In re BitTorrent Adult Film Copyright Infringement Cases, 2012 U.S. Dist. LEXIS 61447, at *9 (E.D.N.Y. 2012); *see also Next Phase Distrib., Inc. v. Does 1-27*, 2012 U.S. Dist. LEXIS 107648, at *14-15 (S.D.N.Y. July 31, 2012)(same). The *In re BitTorrent* court further advised Plaintiff, Malibu Media, LLC, and its counsel in unambiguous terms that:

[It was] concerned about the possibility that many of the names and addresses produced in response to Plaintiff’s discovery request will not in fact be those of the individuals who downloaded “My Little Panties # 2.” The risk is not purely speculative; Plaintiff’s counsel estimated that 30% of the names turned over by ISPs are not those of individuals who actually downloaded or shared copyrighted material. Counsel stated that the true offender is often the “teenaged son ... or the boyfriend if it’s a lady.” Alternatively, the perpetrator might turn out to be a neighbor in an apartment building that uses shared IP addresses or a dormitory that uses shared wireless networks. This risk of false positives gives rise to the potential for coercing unjust settlements from innocent defendants such as individuals who want to avoid the embarrassment of having their names publicly associated with allegations of illegally downloading “My Little Panties # 2.”

Id. (citing *Digital Sin, Inc. v. Does 1-176*, 2012 U.S. Dist. LEXIS 10803, at *3 (S.D.N.Y. 2012)) (citations omitted).

The *In Re Bittorrent* court specifically noted that Plaintiff's original complaint admitted that "IP addresses are assigned to devices" and that, as Plaintiff argued then, that by allowing Plaintiff to discover the individuals associated with those IP addresses, it would "reveal defendants' true identity." *Id.* at *13. The court flatly rejected this flawed reasoning and correctly determine that identification of the actual infringer would be "unlikely" noting that "most, if not all, of the IP addresses will actually reflect a wireless router or other networking device, meaning that while the ISPs will provide the name of its subscriber, the alleged infringer could be the subscriber, a member of his or her family, an employee, invitee, neighbor or interloper." *Id.*

Contrary to Plaintiff's admittedly self-serving "guess," in identical Bittorrent cases across the country courts have overwhelmingly recognized, and numerous plaintiff's have even admitted on the record the simple fact that an IP address does not, and cannot identify an infringer. See *SBO Pictures, Inc. v. Does 1-3036*, 2011 WL 6002620, at *3 (N.D. Cal. 2011) ("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."); *Third Degree Films v. Doe*, 2011 U.S. Dist. LEXIS 128030, *9 (N.D. Cal. 2011) (ISP subscriber information "does not tell Plaintiff who illegally downloaded Plaintiff's works."); *Pacific Century Intern. Ltd., v. Does 1-101*, 2011 2011 U.S. Dist. LEXIS 124518, at *2 (N.D. Cal. 2011) (noting that Plaintiff disavowed previous representations to the court that the requested discovery of subscriber's information based on an IP address would allow it to identify Defendants); *Digital Sin, Inc. v. Does 1-5698*, 2011 WL 5362068, at *4 (N.D. Cal. Nov. 4, 2011) (ISP subscribers may not be the individuals who infringed upon Digital Sin's copyright); see also e.g. *In re: Ingenuity 13 LLC*, No. 2:11-mc-0084-JAM-DAD, Order [Doc. No. 24], at *10 (E.D. Cal. 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"); *In re Ingenuity 13 LLC*, 2012 U.S. Dist. LEXIS 38647, *18 (E.D. Cal. Mar. 20, 2012) (ISP subscriber "information alone 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" and that petitioner "would be required to engage in further pre-filing discovery to determine if a viable cause of action existed against any of the identified subscribers."); *Hard Drive Productions, Inc. v. Does 1-130*, 2011 WL 553960, at *2 (N.D. Cal. 2011)("Plaintiff concedes, in some cases the Subscriber and the Doe Defendant will not be the same individual"); *VPR Internationale v. Does 1-1017*, 2011 U.S. Dist. LEXIS 64656 at *4 (C.D. Ill. Apr. 29, 2011) (noting that "[t]he infringer might be the subscriber, someone in the subscriber's household, a visitor with her laptop, a neighbor, or someone parked on the street at any given moment.").

The United States District Court for the District of Colorado has recognized the results of the simple calculation that an IP address does not equal infringer. As Judge Martinez noted in *Malibu Media, LLC v. Felitti*:

[S]ubscriber John Doe 1 could be an innocent parent whose internet access was abused by her minor child, while John Doe 2 might share a computer with a roommate who infringed Plaintiffs' works. John Does 3 through 203 could be thieves, just as Plaintiffs believe."
2012 U.S. Dist. LEXIS 103393, at *9-10 (D. Colo. July 25, 2012)(quoting *Third Degree Films v. Does 1-3577*, 2011 U.S. Dist. LEXIS 128030, at *4 (N.D. Cal. Nov. 4, 2011)). Judge Martinez even went so far as to note the effects of this disconnect between internet subscriber and actual infringer disclosing that:

The Magistrate Judge assigned to all BitTorrent cases has noted that defendants are coming forward with a multitude of different defenses. Some are businesses alleging that a patron was the unlawful downloader. Others are elderly grandparents that do not even know what BitTorrent is or how to download a file from the internet; they may have owned the computer associated with the unique IP address, but have no knowledge of whether someone in their household may have used the BitTorrent protocol for the purposes alleged in the complaint."
Id.

Despite the overwhelming and specific findings and admissions to the contrary, Plaintiff admittedly named the Defendant as the alleged infringer simply because his name is on the cable bill. (Complaint ¶19). This central allegation is merely a guess. This legal fiction has been resoundingly rejected by this and numerous other courts. Rule 8(a)(2) requires more. It requires

Plaintiff to plead facts sufficient to allow the court to draw the reasonable inference that the defendant was the person who actually engaged in the alleged infringing activity. Plaintiff has 221222222022212222221222223224225226227228229221022112212221322142

B. PLAINTIFF FAILS TO ALLEGE FACTS THAT DEFENDANT COMMITTED A VOLITIONAL ACT OF COPYRIGHT INFRINGEMENT

Consistent with its burden under Fed.R.Civ.P. 8(a)(2), Plaintiff must plead facts sufficient to allow the Court to draw the inference that the Defendant violated one or more exclusive rights set forth in 17 U.S.C. §106. *See, Feist, supra*. 499 U.S. at 361. While copyright is a strict liability statute, many courts have correctly recognized that inherent in any such violation of a §106 right, some element of volition or causation must exist. *See Religious Tech. Ctr v. Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1369-70 (N.D. Cal. 1995) (granting motion to dismiss where Plaintiff failed to plead any plausible facts that Defendant committed a volitional act of copyright infringement.); *see also Field v. Google, Inc.*, 412 F. Supp. 2d 1106 (D. Nev. 2006) (holding that a plaintiff must show volitional conduct on defendant's part to support finding of direct copyright infringement); (*Cartoon Network LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008)(holding that under section §106 of the Copyright Act a person must "engage in volitional conduct - specifically, the act constituting infringement - to become a direct infringer"). This is especially instructive as no automated or electronic process is alleged to have executed the infringing activity. Nor does Plaintiff's allege any claims for secondary liability. For Defendant to have infringed Plaintiff's work in the manner alleged, he would have had to consciously and physically execute numerous physical steps to accomplish such an action.

It stands to reason that, as shown above, since an IP address cannot identify a person, it certainly cannot identify a person that actually committed an volitional act of direct infringement. To hold otherwise would result in an absurd result that is contrary to the Federal Rules, justice and common sense. Plaintiff's conclusory allegation that whoever paid the internet bill is the infringer meaning that he/she physically engaged in a volitional act of copyright is legally insufficient to support a claim upon which relief may be granted. Significantly, as it has already been shown, Plaintiff cannot even identify who may have infringed its works, if such a person

even exists, it certainly has not plead any facts supporting an inference that Defendant actually engaged in any volitional infringing activity, and thus lacks a good faith basis for asserting copyright infringement claims against Defendant.

**C. PLAINTIFF'S SUPPORTING EVIDENCE IS INACCURATE.
MISLEADING AND NOT OFFERED IN GOOD FAITH**

Plaintiff's Complaint consists of a series of conclusory statements arranged to support the already speculative conclusion that whoever pays the internet bill is the infringer. As noted above, these claims find sole support in a boilerplate information from IPP, Limited that does not specifically identify the Defendant or accuracy of their method² While the Plaintiff generally describes how BitTorrent work to transmit data the information provided by Plaintiff includes no information other than their belief that such steps were taken in this matter. For example, despite acknowledging that "ISPs keep track of the IP addresses assigned to their subscribers" the Plaintiff does not state that any ISP was ever contacted regarding this matter. There is no information provided is the defended was a member of the swarm for 1 second or the full 6 weeks or copied 0, 1, or all parts of the file. In short, the Plaintiff provides no basis whatsoever to support the Plaintiff's conclusion that Defendant is the "subscriber of the IP address" used in connection with committing the allegedly infringing acts, actually copied data or obtained a usable copy of any part of the work. In addition, and perhaps more fatal to Plaintiff's allegations, the information provided is inaccurate and misleading as the actual nature of IP addresses and their inability to identify an alleged infringer. Each of these defects will be taken up in turn:

First, the Plaintiff states that an "An IP address is a number that is assigned by an Internet Service Provider("ISP") to devices, such as computers, that are connected to the Internet.

(Complaint. ¶18). However, this is incorrect and misleading. As previously described, any subscriber of an ISP, such as Defendant, who connects their computer to the internet via the ISP, for example through a wireless router, is assigned an Internet Protocol (IP) address. *Kirch*, 2011

² It is also commonly know that firms such as IPP, Ltd., have a direct financial interest in the outcome of case where they provide evidence undermining the credibility of the Plaintiff declaration. *See e.g. Metso Minerals, Inc. v. Powerscreen Int'l Distrib. Ltd.*, 833 F. Supp. 2d 282, 316 (E.D.N.Y. 2011) (Court determined declarant lacked credibility due to direct financial interest in the action).

U.S. Dist. LEXIS at *10. As noted above, the purpose of an IP address is to route traffic efficiently through the network. IP addresses only specify the locations of the source and destination nodes in the topology of the routing system. As such, as an IP address, as described above, is not assigned to an "internet user" but merely an internet access point such as a wireless router. *In Re: BitTorrent*, 2012 U.S. Dist. LEXIS 61447 at *13. ("[m]ost, if not all, of the IP addresses will actually reflect a wireless router or other networking device). Furthermore, as detailed above, an IP address simply cannot identify a computer being used nor the actual user. *Id.* at *9. Plaintiffs unsupported and misleading conflation between Defendant/subscriber with an actual infringer/user -- if such a person even exists -- cannot rise above merely a speculative claim for relief against Defendant and Plaintiff's claims should be dismissed.

Second, no good faith basis exists for the Plaintiff statement that the information listed in Exhibits A of the Complaint "show: Each Defendant had copied a piece of Plaintiff's Copyrighted Work." The Plaintiff goes onto to make the unsupported statement that "Therefore, each Defendant was part of the same series of transactions." participating in the alleged infringing activity, (*complaint* ¶139), and that the ISP can "correlate the Defendant's IP address to the Defendant's true identity" (*Complain* ¶19). Again, these statements are incorrect and misleading and not offered in good faith. As exhaustively pointed out an IP address can neither identify an individual nor a specific computer, let alone Defendant's computer, or any specific computer accessing the internet. *See, In Re: BitTorrent*, 2012 U.S. Dist. LEXIS 61447 at *13. ("Most, if not all, of the IP addresses will actually reflect a wireless router or other networking device, meaning that while the ISPs (sic) will provide the name of its subscriber, the alleged infringer could be the subscriber, a member of his or her family, an employee, invitee, neighbor or interloper.").

There exists no reasonable good faith basis upon which the Plaintiff could state that the Defendant, based on an IP address alone infringed on anyone's work(s). In an identical Bittorrent case, two separate declarations -- herein referred to as Exhibit B and incorporated in their entirety by reference -- provided by experienced and qualified computer science professionals confirm that there is no way that a person in IPP Limited or Plaintiff's position could have made the aforementioned claims in good faith. (Decl. Stephen Hendricks ¶10). Indeed, both declarations confirm that it would be impossible to make any

such determination. (Decl. Stephen Hendricks ¶10; Decl. John Simek ¶16).³ Such inaccurate and misleading evidence offered in bad faith cannot support Plaintiff's claims and its Complaint should be dismissed.

Third, the Plaintiff conclusory and unsupported argument that the Defendant: 1) committed an act of infringement, 2) using his computer; and that he 3) can be identified fails as a matter of fact. For example, a subscriber can be misidentified in multiple ways as an infringer without participating in any infringing behavior, including at least:

1. Some members of a swarm simply and automatically pass on routing information to other clients, and never possess even a bit of the movie file;⁴
2. A client requesting a download can substitute another IP address for its own to a Bittorrent tracker;⁵
3. A user can misreport its IP address when uploading a torrent file. A user in the network path between the user monitoring IP address traffic and the Bittorrent tracker can implicate another IP address;⁶
4. Malware on a computer can host and distribute copyrighted content without knowledge or consent;⁷
5. There are reliability issues with using IP addresses and timestamps to identify the correct party;⁸

address "spoofing" refers to the creation of a forged IP address with the purpose of concealing the user's identity or impersonating another computing system.). 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.

³ Similar to the Defendant referenced in both the Hendricks and Simek declarations, Defendant's ISP is Comcast

⁴ Sengupta, S. et al., Peer-to-Peer Streaming Capacity, IEEE Transactions on Information Theory, Vol. 57, Issue 8, pp. 5072-5087, at 5073 (Prof. Helmut Bolcski, ed., 2011) ("A [BitTorrent] user may be the source, or a receiver, or a helper that serves only as a relay.")

⁵ Michael Piatek et al., *Challenges and Directions for Monitoring P2P File Sharing Networks—or—Why My Printer Received a DMCA Takedown Notice*, 3 (2008), http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf See also, "IP address spoofing" http://en.wikipedia.org/wiki/IP_address_spoofing (Last visited August 2, 2012) (the term IP

⁶ Ibid.

⁷ Ibid.

⁸ Ibid. ("When IP addresses are assigned dynamically, reassignment of an IP address from an infringing user to an innocent user can cause the behavior of the infringing user to be attributed to the innocent

6. If a subscriber has dynamic IP addressing through its website host, it is sharing an IP address with several other subscribers;⁹

7. Anyone with wireless capability can use a subscriber's "wi-fi" network to access the Internet, giving the impression that it is the subscriber who is infringing;¹⁰ or

8. Human error by IPP, Ltd, Plaintiff and/or the ISP among others.

All of the above footnoted information is publically available and may be considered by this Court. See *Grynberg v. Koch Gateway Pipeline Co.*, 390 F.3d 1276, 1279 n.1 (10th Cir. 2004)(in ruling on a Rule 12(b)(6) motion to dismiss, a court may properly consider facts subject to judicial notice such as court files and matters of public record)(citations omitted).

Such facts do not exist in a vacuum. By defining Doe Defendants as ISP subscribers who were assigned certain IP addresses, instead of the actual Internet users who allegedly engaged in infringing activity, "Plaintiff's sought-after discovery has the potential to draw numerous innocent internet users into the litigation." *Hard Drive Prods., Inc. v. Does 1-130*, No. C-11-3826 DMR, 2011 U.S. Dist. LEXIS 132449, at *6 (N.D. Cal. Nov. 16, 2011)).

Recent court decisions have expressed strong concerns along these lines about the coercive nature of copyright claims based on Bittorrent identification and especially involving pornographic material. *In re Bittorrent*, supra, 2012 WL 1570765 at *10 ("This concern, and its potential impact on social and economic relationships, could compel a defendant entirely innocent of the alleged conduct to enter an extortionate settlement"); *SBO Pictures, Inc. v. Does 1-3036*, 2011 U.S. Dist. LEXIS 137361, at *11 (N.D. Cal. Nov. 30, 2011) (a defendant – "whether guilty of copyright infringement or not -- would then have to decide whether to pay money to retain legal assistance to fight the claim that he or she illegally downloaded sexually

user. Because the monitoring client (copyright holder) records information from the tracker of the Bittorrent client, the information can quickly become inaccurate and will not implicate the correct user.")

⁹ "Web hosting service" http://en.wikipedia.org/wiki/Web_hosting_service (Last visited August 2, 2012).

¹⁰ Carolyn Thompson writes in an MSNBC article of 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 IP subscribers' Wi-Fi connections (including a secure connection from the State University of New York). See Carolyn Thompson, *Bizarre Pornography Raid Underscores Wi-Fi Privacy Risks* (April 25, 2011), www.msnbc.msn.com/id/42740201/ns/technology_and_sciencewireless/

explicit materials, or pay the money demanded. This creates great potential for a coercive and unjust 'settlement'); *See also Zero Tolerance Entertainment, Inc. v. Does 1-45*, 2012 WL 2044593 at *1 (S.D.N.Y. Jun. 6, 2012) (discovery of ISP subscriber information "has been used repeatedly in cases such as this one to harass and demand of defendants quick settlement payments, regardless of their liability").

Defendant does not argue that Plaintiff has no right to enforce a valid copyright in accordance with the laws and procedures of this Court, however, such claims must comport with the pleading and evidentiary standards of those same laws. It has not, and its Complaint should be dismissed.

D. COUNSEL IN IDENTICAL CASES HAVE ADMITTED ON THE RECORD THAT THERE EXISTS A SIGNIFICANT RISK OF MISIDENTIFICATION

The increasing popularity of wireless routers through which unknown interlopers can access subscribers' internet accounts, *In re Bittorrent*, supra, 2012 WL 1570765 at *3, makes the allegation that the subscribers committed the infringement in this case all the more speculative. The Court should not close its eyes to the significant risk that people innocent of any copyright infringement are being falsely identified as "Defendants" and swept up in such BitTorrent lawsuits. Specifically, in an age when most homes have routers and wireless networks and multiple computers share a single IP address "there is a reasonable likelihood that the [defendants] may have had no involvement in the alleged illegal downloading that has been linked to his or her IP address." *Malibu Media, LLC v. John Does 1-11*, 2012 U.S. Dist. LEXIS 94648 (D.D.C. July 10, 2012).

Various plaintiffs in identical Bittorrent cases have even admitted on the record that ISP subscriber information is insufficient to identify and name an alleged infringer. Indeed, as one judge observed in another of identical Bittorrent case, plaintiff's counsel admitted in open court that:

30% of the names turned over by the ISP's are not those of the individuals who actually downloaded or shared copyrighted material.

Digital Sin, Inc. v. Does 1-176, 279 F.R.D. 229, 242 (S.D.N.Y. 2012) citing (1/17/12 Tr. at 16)

(emphasis added); *see also Pacific Century Intern. Ltd., v. Does 1-101*, 2011 U.S. Dist. LEXIS 124518, *2 (N.D. Cal. 2011)(noting that Plaintiff disavowed previous representations to the court that the requested discovery would allow it to "fully identify" Defendants and further admitting that the discovery often will not reveal Defendants' identities); *AF Holdings LLC v. Does 1-96*, 2011 U.S. Dist. LEXIS 134655, at *11-12 (N.D. Cal. Nov. 22, 2011)(plaintiff conceded on the record that "the [ISP subscriber] information subpoenaed will merely reveal the name and contact information of the subscriber to the Internet connection that was used to download the copyrighted work, but it will not reveal who actually downloaded the work and therefore who can be named as a defendant.")

Instructive also is *Boy Racer, Inc. v. Doe*, 2011 U.S. Dist. LEXIS 103550 (N.D. Cal. Sept. 13, 2011). Here the plaintiff in identical Bittorrent case admitted that its previous representation to the court that ISP subscriber information was not sufficient to "fully identify" a P2P network user suspected of violating the plaintiff's copyright was false and instead that still more discovery would be required to identify the actual infringer. *Id.* at *6-7. The Plaintiff in that case specifically stated on the record that:

While Plaintiff has the identifying information of the subscriber, this does not tell Plaintiff who illegally downloaded Plaintiff's works, or, therefore, who Plaintiff will name as the Defendant in this case. It could be the Subscriber, or another member of his household, or any number of other individuals who had direct access to Subscribers network.

Id. Needless to say the *Boy Racer* court found this "turn of events troubling, to say the least." *Id.* at *7-8.

Even more instructive for this Court, in another identical Bittorrent case, plaintiff's counsel, in seeking to address the Court's concern that it may be pursuing and innocent internet subscribers admitted in court documents that it would require additional discovery before it could determine if the subscriber was in fact one in the same stating that:

Although a subscriber and doe defendant will often be one-and-the-same, it can be the case that they are different people. In cases, such as the present action, where the subscriber completely refuses any form of communication with Plaintiff's counsel, limited additional discovery is often needed to confirm that the subscriber may be named as a Doe Defendant.

Further stating that:

"[a]fter making its determination [through additional deposition discovery] as to the correct Defendant, Plaintiff will effectuate service."

Hard Drive Prod's. v. Doe, N.D. Cal. Case No. 22-1566, Status report filed by Brett Gibbs: Dkt.

No. 29, 11/11/11). See Section III(c), *infra*. Similar to the 30% error rate admitted in the *Digital Sins* court, here plaintiff's counsel, operating under nearly identical facts admits that in order to have a good faith basis to allege that an Internet subscriber is actually a Defendant; it needs to know more than that the person happens to pay the bill. *Id.*¹¹

Such admissions provide further support that Plaintiff's unsupported "guess" that Person that is paying the internet bill is the infringer in this case is utterly speculative, and the complaint is thus subject to dismissal, as: 1) Plaintiff admittedly does not know who actually committed the alleged infringement (Complaint, ¶¶ 7) the Complaint alleges no facts supporting an inference that the subscriber of the account, i.e., the Defendant who merely pays the bill for the account, is in fact the individual who actually uploaded or downloaded Plaintiff's movie; and 3) the Complaint alleges no basis for holding an account subscriber liable for the allegedly infringing conduct of unknown others, even if such person(s) even existed.

E. PLAINTIFF'S ALLEGATIONS ARE LIKELY UNSUPPORTABLE UNDER EVEN RULE 11

Plaintiff conclusory allegations that Defendant, as merely an internet subscriber is the the infringer is likely not even supportable under Fed.R.Civ.P. 11, let alone Fed.R.Civ.P. 12(b)(6).¹² Specifically, naming an internet account subscribers as a Defendant – without any evidentiary basis for claiming that the subscribers actually committed the alleged infringement – likely violates Rule 11's requirement that "the factual contentions (i.e., that the defendant in this case was personally involved in uploading and downloading copyrighted

¹¹ These aforementioned admissions may be judicially noticed by this Court. See generally *St. Louis Baptist Temple v. FDIC*, 605 F. 2d 1169, 1171-1172 (10th Cir. 1979) ("federal courts, in appropriate circumstances, may take notice of proceedings in other courts, both within and without the federal judicial system, if those proceedings have a direct relation to matters at issue.").

¹² Counsel for Defendant has been authorized to evaluate the possibility of seeking sanctions under Rule 11 and other bases and will proceed appropriately.

material) have evidentiary support . . .” An attorney’s signature on a motion or pleading means “that to the best of his or her knowledge, information, and belief there is good ground to support the contentions in the document, both in terms of what the law is or should be and in terms of the evidentiary support for the allegations, and that he or she is acting without an improper motivation.” Charles Alan Wright & Arthur R. Miller, *5A Fed. Prac. & Proc. Civ.* § 1335 (3d ed.).

Plaintiff, Malibu Media, LLC, has been specifically warned in an identical Bittorrent case of the potential for sanctions for incorrectly identifying and naming defendants. *See Malibu Media, LLC v. Doe*, 2012 U.S. Dist. LEXIS 110668, at *6-7 (M.D. Fla. Aug. 7, 2012) (“The plaintiff shall inform each John Doe defendant of the potential for sanctions under Rule 11, Fed.R.Civ.P., if the John Doe defendant is incorrectly identified”); *see also e.g. Hard Drive Productions v. Does 1-48*, No. 11-9062, 2012 U.S. Dist. LEXIS 82927, 2012 WL 2196038, *6 (N.D. Ill. June 14, 2012) (warning plaintiff to consider Rule 11 before naming defendant who disputed that he had illegally downloaded pornographic movie). As another court recognized earlier this month, subscribers to internet accounts may be made defendants in these kinds of cases only “on the basis of their allegedly infringing activity, not due to their status as subscribers of the IP address utilized.” *Discount Video Center, Inc. v. Does 1-29*, 2012 U.S. Dist. LEXIS 112518, at *5 n. 7 (D. Mass. Aug. 10, 2012).

Indeed, public records indicate that Plaintiff, Malibu Media, LLC, has filed approximately 355 lawsuits since February of this year, implicating what is believed to be approximately 5000 individuals or businesses. Assuming the generous estimate of a 30% false positive rate, the potential exists for approximately ~1700 defendants to be wrongful caught up in such suits. Coupled with Plaintiff’s consistent refusal to accept exculpatory evidence from similar Defendants — and other similarly situated individuals as demonstrated in Exhibit A, supports a conclusion that Plaintiff’s conclusory allegations lack evidentiary support and as such cannot rise above mere speculation warranting dismissal.

F. COMCAST (THE ISP) ASSIGNMENT OF IP ADDRESS IS BY DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SO IT DYNAMICALLY CHANGES FOR EACH USER

Comcast the ISP for John Doe 16 uses Dynamic Host Configuration Protocol to assign their IP address as they do for most subscribers. "Dynamic" mean that the IP address assigned to its subscribers changes from time to time. These IP changes can happen at any time either by the ISP provider, or by the defendant, or automatically. There is no indication by the Plaintiff that they tracked the IP address of each defendant over the period of the alleged swarm. There is no indication how long the defendants were a part of the swarm. The defendant IP address may have been reused by the ISP multiple times during the 5 week period of the alleged swarm. The plaintiff has not provided information that demonstrates that the process used to capture IP address also prevents capturing IP address of incident John Doe that happen to be assigned the previous IP address of a copyright infringer that was a part of the alleged swarm.

G. VENUE DETERMINED BY GEO LOCATION INFORMATION IS INHERENTLY INACCURATE

In United States District Court Southern District of New York (combat Zone corp., vs. Does 1-34, 12 Civ. 4133 (CM) Honorable Judge McMahon explained:

Third, counsel has not satisfied the court that all 34 John Doe defendants are amenable to suit within this district. Counsel says, "Plaintiff has listed only John Does *who are believed to be* within the District of this Court," based on geolocation data that he admits "are not 100% reliable." (Pl. Response to Order to Show Cause at 3). But this court already knows, from *Digital Sin*, that there are serious problems with plaintiff's approach to in personam jurisdiction. In *Digital Sin*, I allowed plaintiff to proceed against John Doe 1 (after severing the other 246 John Does), *only to have plaintiff's counsel file a discontinuance in short order; the cited ground was that plaintiff had learned that John Doe 1 – his geolocation data notwithstanding – was not a New York resident and was not amenable to suit in the Southern District of New York!* I commend counsel for his candor in admitting the want of jurisdiction once it was uncovered, but he makes my point: the amenability of these defendants to suit in this district is suspect.

Likewise in this case the geo location provided for John Doe 16 is wrong as the residence is not in La Grange Park IL.

H. HASH VALUE IS NOT A FINGERPRINT OF SENDER AND RECIPIENT

The Plaintiff in their (Complaint ¶122) quotes "In this way, the hash identifier works like an electronic fingerprint to identify the source and origin of the piece and that the piece is authentic and

uncorrupted.” This statement is incorrect and misleading the court. The hash value in question 5D078FC4F665E7B3E7D80C47845956542379750F identify the total torrent file and provides a way to identify if the complete torrent file was corrupted in transmission but it does not in any way identify the source or origin of the pieces of the file. In fact if the court searches the internet today for the same hash value in question they will find hundreds of sites allowing the exact same hash file to be downloaded and some of those sites will indicate that the same hash value is being actively downloaded by dozens of users currently. The hash value is not unique to this group of defendant’s proposed activity. All users in the world downloading the same torrent file will use the same hash value.

I. No evidence that UPLOADING OR DOWNLOADING OF COPYRIGHT WORK OCCURRED

The Plaintiff indicates that each Defendant had copied a piece of Plaintiff copyrighted work identified by the Unique Hash Number. The Unique Hash Number only indicates the unique Hash # of the complete file and not the hash values of the parts of the file. This file in question potentially has thousands of parts, each with a unique Hash #. There is no information provided by the plaintiff as to what if any of the thousands parts of the file were transmitted or received from or to any of the defendants or if any of the defendants actually received or retransmitted a part successfully to each other or anyone else. Each piece of the file is not usable without all the parts of the torrent file. It is as if receiving a DVD with multiple wedge shaped parts cut out. The DVD is useless without all the parts. It is the very nature of a bit torrent that torrent members come and go from the swarm. There is no indication that all the Doe’s in this case were a part of the swarm from the start to the end of time period indicated 7/31/2012, 15:31 UTC to 9/5/2012, 2:19 UTC. In fact the swarm is continuing as you read this as indicated by the Hash # still being readily available by performing a search for the Hash # using www.Google.com. There is no information provided by the Plaintiff that any of the Does in this case transmitted a complete useable copy of the work in question or a playable part of the work in question. The Plaintiff alleges that the Does connected to a swarm with a particular Hash value. We do not know if that was for 1 second, 1 hour, or 5 weeks continuously as provided by the plaintiff as the start and end of the swarm. Only 2 out of the 23 Does were even connected to the swarm on the same day and none were connected on the same time according to the Plaintiff making it impossible for the Does to share any information or concluded with each other since they were not a part of the swarm at the same time as indicated by the Plaintiff.

J. COUNT 1 DIRECT INFRINGEMENT AGAINST DOES 1-23

(Complaint ¶147) “By using the BitTorrent protocol and a BitTorrent Client and the processes described above, each Defendant copied the constituent elements of the registered Work that are original.” There is no indication or evidence from the Plaintiff that the Doe’s copied parts of the proposed registered work. The information provided by the Plaintiff indicates that the Plaintiff agent IPP Limited was able to join a BitTorrent swarm and build a copy of the Plaintiff’s work. There is no indication that all or parts of the “work” came from these Doe’s or some other members of the swarm still in operation. There is no information provided by the Plaintiff saying if the Plaintiff only copied the metadata of the file and not the actual torrent file. The only thing the Plaintiff indicates is that the Plaintiff was able to use BitTorrent to obtain a copy of its copyrighted material but from who as identified by either a IP address or person is unknown. It is entirely possible the Plaintiff agent IPP Limited received all of the alleged parts of the torrent from swarm members that are not a part of this litigation and not located in Illinois or the United States.

K. THE PLAINTIFF “WORK” THAT IT ALLEGES ITS COPYRIGHT WAS INFRINGED UPON BY THE DEFENDANTS IS READILY AVAILABLE ON ITS ASSOCIATED WEB SITE X-ART.COM FOR FREE.

(Complaint ¶148) “Plaintiff did not authorize, permit or consent to Defendants’ copying of its Work” The Plaintiff Work “Transcendence” movie, the subject of this litigation is available free on the plaintiff owners own site at this location <http://hosted.x-art.com/galleries/transcendence/index.php?PA=2081011> in a lower resolution version as well as affiliate sites as a sort of advertisement promoting its works and attempting to attract potential subscribers. These adult advertisements are viewable by anyone simply visiting the URL. A search for the work in question on a popular web search engine (www.google.com or www.bing.com) will return multiple sites showing said work as an advertisement to join the Plaintiff controlled subscription based web site X-Art.com to see the full version of the movie. It is possible that one or more of the Does in this case believed they were downloading one of the advertisements using BitTorrent if they downloaded anything. In addition, in order to gather the information presented in the complaint the Plaintiff’s IPP Limited firm participated in the swarm by exchanging information with swarm members if not file parts facilitating the alleged infringement of the alleged copy protected work.

K. PLAYABLE WORK?

There is also no indication from the Plaintiff that the defendant's had a playable copy of the Plaintiff work. Even if the defendant's had 99% of the Plaintiff work the defendant would not be able to play any part of the work. Without being able to play the plaintiff work the defendant would not be able to know if they had a copyrighted work or some other file with the same name. Even today the Defendants may not have completed the download of all parts of the torrent in question and still don't know if they have a copyrighted work or not because they can't play it. In addition if you go to the torrent websites indicated by the Plaintiff (www.btscene.com and www.extratorrent.com) you will find 18 different torrent downloads with the word Transcendence in the name. None of the works are called "Transcendence" exactly. A search of the United State Copyright office for the names indicated on the torrent web sites returns 0 results for copyrighted material. Without completing the download and recompilation of the parts and then successfully opening and viewing the file for copy right information the defendant's would not have known what they actually download or if it was a copyrighted or public "advertisement".

L. QUALIFICATIONS OF IPP, LIMITED ("IPP")

The Plaintiff indicated that they retained IPP, Limited ("IPP") to identify the IP address of the defendant's. There is no information provided as to who IPP, Limited is; what their address is; or what their qualifications and experience are; or if their investigative techniques have stood up to challenges in a US Court or by peers. Therefore there is no basis to determine the accuracy of the IP address, the times they were used, or location as provided by the Plaintiff.

M. VALIDITY FOR THE SOFTWARE "INTERNATIONAL IPTRACKER V1.2.1"

The Plaintiff indicates that (Complaint ¶137) "IPP used forensic software named INTERNATIONAL IPTRACKER v1.2.1 and related technology enabling the scanning of peer-to-peer networks for the presence of infringing transactions." There is no indication of an independent peer review of the software "INTERNATIONAL IPTRACKER v1.2.1" its methods and amount of accuracy it may or may not have. There is no indication that the software techniques have stood up in a US Court as accurate and admissible. The software is not available for purchase for independent review. Therefore there is no

basis to determine the accuracy of the IP address, times they were used, or there locations, as provided by the Plaintiff.


N. MOTIVE OF ATTORNEY

(Complaint ¶144) . Plaintiff retained counsel to represent it in this matter and is obligated to pay said Counsel a reasonable fee for its services.” It is suggested to the court to inquire what is the “reasonable fee” in this case as it has been alleged in similar cases the typical agreement is for the Plaintiff attorney to receive 90% what is recovered through settlements or litigation to cover the cost and pursue these allegations and the Plaintiff would receive 10% for the use of their alleged copyright. It is interesting that the Plaintiff a California company would hire a Michigan based attorney that was sanctioned in Michigan for filling a frivolous defense¹³ and frivolous lawsuit¹⁴ to try an Illinois case.

III. CONCLUSION

Plaintiff’s allegations against the Defendants in this case are premised on the mere possibility that they might have been the infringing individual. Such conjecture, based solely on Defendants status as the internet accountholder, is exactly the kind of speculative pleading that is barred by *Twombly*, *Iqbal*, and their progeny. Plaintiff cannot just guess, as it does in its Complaint, that defendant is the most likely infringer because it doesn’t have any factual basis to name anyone else. The Complaint must therefore be dismissed for failure to state a claim. Defendant further requests that the Court retain jurisdiction as to the issue of awarding attorneys fees and costs, including imposition of sanctions under Fed.R.Civ.P. 11, and other bases.

Respectfully submitted December 21, 2012.


John Doe #16

¹³ State of Michigan Court of Appeals, Wayne Circuit Court No. 232266; LC No. 00-000978-PD

¹⁴ State of Michigan Court of Appeals, Lapeer Circuit Court No. 188674 LC No. 95-021074-CK

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM UPON WHICH RELIEF CAN BE GRANTED, was served by Us Mail to the court and Plaintiff counsel:

Paul Nicoletti, Esq.

Law offices of Nicoletti & Associates, LLC

36880 Woodward Avenue, Suite 100

Bloomfield Hills, MI 48304

Exhibit A

Eastern District Of Pennsylvania

Malibu Media, LLC

v.

John Does 1-14

Case No. 2:12-CV-02084

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

MALIBU MEDIA, LLC,
Plaintiff,

CASE No. 2:12-CV-02084

v.

JOHN DOES 1-14,
Defendants.

**DECLARATION TO REFUTE INFORMATION PROVIDED BY PLAINTIFF'S
COUNSEL, CHRISTOPHER FIORE, 14 MAY 2012 HEARING**

I, an anonymous John Doe, do hereby declare:

1. I'm over 18 years of age and competent to make this declaration.
2. I have personal knowledge of the facts in this declaration and the information provided by Plaintiff's counsel, Christopher Fiore, on 14 May 12 (Document #6), during the motion hearing for cases 2:12-CV-02078, 2:12-CV-02084, and 2:12-CV-02088 (Malibu Media LLC is the Plaintiff for these cases), in support of Plaintiff's motion for leave to take discovery prior to Rule 26(f) conference.
3. I have also sent six previous declarations (October 2011 – January 2012) for copyright infringement cases for various courts: Eastern District of Virginia (Richmond Division), *3:11-cv-00531-JAG (Patrick Collins v. Does 1-58)*, *3:11-cv-00469-JAG (K-Beech v. Does 1-85)*, District of Arizona, *2:11-cv-01602-GMS (Patrick Collins v. Does 1-54)*, the Northern District of Florida, *4:11-CV-00584 (Digital Sin, Inc., v. Does 1-145)*, Northern District of Illinois, *1:11-CV-09064 (Pacific Century International v. Does 1-31)*, and the District of Columbia, *1:12-cv-00048 (AF Holdings, LLC, v. Does 1-1058)*, refuting various Plaintiff

memorandums. Note: Four of the six declarations were accepted by the courts.

4. I'm filing this declaration anonymously, as I'm one of the 200,000+ John Doe defendants in the increasing number of copyright infringement cases filed throughout the U.S.¹ If I were to file this declaration under true name, I feel I would be singled out for vindictive prosecution by my Plaintiff and the network of copyright infringement lawyers that file these types of cases. The case I was under has been dismissed, but like many other Doe defendants, I'm waiting for the statute of limitation to expire. The declarations I have previously filed, and information I provide to Doe defendants on my Web site (<http://diertrolldie.com>), have caused copyright infringement lawyers and Plaintiffs more work and the doubtless loss of settlement fees. To prevent identification, I will be mailing this declaration to the court and Plaintiff from a State other than my own.
5. Plaintiff will likely claim I have no standing to make this declaration, as I'm not one of the Doe defendants in this case. I believe I do have standing and valuable information concerning the information Mr. Fiore provided the court at the 14 May 12, hearing. As the hearing only sought clarification from Mr. Fiore, it is understandable the court would take his responses at face value. My standing is based on my direct knowledge of these types of cases and the operations of computer networks, to include small home/office networks, most (if not all) are what Plaintiff has listed as Doe defendants. I have gathered this knowledge first hand by working as a certified Information Technology Specialist, as a Doe defendant, and by running my Web site (<http://diertrolldie.com>), dedicated to posting news and views concerning copyright infringement lawyers (AKA: Copyright Trolls) and John/Jane Does. While running my site, I have corresponded with many Doe defendants who like myself, are

¹ US News and World report, 2 Feb 12, Jason Koebler, *Porn Companies File Mass Piracy Lawsuits: Are You At Risk?*

<http://www.usnews.com/news/articles/2012/02/02/porn-companies-file-mass-piracy-lawsuits-are-you-at-risk>.

being abused by Plaintiffs and copyright infringement lawyers who follow this business model. Some of the Doe defendants I have interacted with have been pressured to settle with clients of Mr. Fiore for cases filed in the Eastern District of Pennsylvania.

6. I hope my declaration will aid the Court in understanding the questionable practices of Plaintiff, copyright infringement lawyers in general, and correcting the information Mr. Fiore presented the court during the 14 May 12, hearing. The anonymous nature of this declaration does not detract from its logic, truthfulness, and will only aid in the understanding of these technically complex types of cases. I thank the court for indulging this John Doe.

7. BitTorrent

BitTorrent is a computer program and protocol (system of rules) for sharing large files across the Internet. BitTorrent is part of a group of file sharing applications, known as peer-to-peer (P2P). BitTorrent is completely legal and only a tool in which the individual user decides how it is used. The company was founded in 2004 and their main office is located in San Francisco, CA. Details concerning BitTorrent can be found at www.bittorrent.com. BitTorrent can and is used by personnel engaged in illegal file sharing, to include Plaintiff's movies. It is also used to legally distribute various files, to include software, music, ebooks, and movies. The BitTorrent Company and the various versions of its file sharing software are not hidden in some basement in Eastern Europe or Asia as Mr. Fiore suggests. This statement makes it seem that Mr. Fiore has very little knowledge on the software that plays a central part in these copyright infringement cases he is filing.

8. Wireless Networking

Mr. Fiore claims all the Doe defendants (public IP addresses) had to take active steps to install the BitTorrent software on their computers and was not an accidental matter.

Mr. Fiore omits to tell the court the public IP address Plaintiff's agents recorded does not necessarily correlate to the BitTorrent software being installed on any computer belonging to Doe defendants. The public IP address Plaintiff provided the court only correlates to the immediate location of the Internet service and who pays the Internet Service Provider (ISP). This is due to the fact that a majority of homes and small businesses today use a Wireless Firewall/Router (WFR) to share the Internet connection to systems at their location. The WFR allows multiple wired and wireless connections from computers (some possibility unauthorized); all using the same Public IP address Plaintiff has collected (Exhibit A). As the wireless signal of the WFR commonly extends outside the residence, it is not unusual for unauthorized systems to connect to it. Some ISP subscribers (Doe defendants) may have run their wireless Internet connection open (no password required), so anyone could have connected to it and downloaded Plaintiff's movie. Even if an ISP subscriber secures the wireless Internet connection with a password, there are various vulnerabilities that could be exploited to gain access to it.

Possible claims of negligence on the part of Doe defendants in not securing an Internet connection or by not monitoring what occurs on it are baseless. There is no legal duty or contractual obligation between the defendants and Plaintiff to require such action. On 30 Jan 12, Judge David Ezra, stated the following concerning negligence claims in copyright infringement case 1:11-cv-00262, Liberty Media Holdings, LLC, v. Hawaii members of swarm...,

The Court concludes that the allegations in the FAC are not sufficient to state a claim for negligence for a couple reasons. First, nowhere in the FAC does Plaintiff assert any specific legal duty in connection with its negligence claim. Further, Plaintiff has not cited, nor has the Court found, any case law with analogous facts from which the Court could conclude that the Defendants owed Plaintiff a general duty to secure their internet connection. Second, even assuming

Plaintiff had alleged a cognizable duty, the FAC fails to allege any facts demonstrating how Plaintiff breached that duty. Plaintiff's Memorandum in Opposition to the instant Motion highlights the purported risks associated with failing to password-protect one's wireless network. However, Plaintiff does not allege in the FAC that any of the individual Defendants failed to password-protect his/her wireless network or otherwise monitor the use of his/her computer by others. The bare assertion that they "failed to adequately secure their Internet access" is conclusory and unsupported by specific factual allegations regarding the individual Defendants. Therefore, it is not entitled to an assumption of truth for purposes of ruling on the instant Motion. (*1:11-cv-00262-DAE-RLP, Document #66, Order: (1) Granting in Part and Denying in Part Defendant Hatcher's Motion to Dismiss, (2) Granting Plaintiff's Leave to Amend, and (3) Vacating the Hearing, Page 13*)

The WFR provides each system connected to it an "internal" IP address that no one outside the home network will ever see (Exhibit A). The unauthorized use of a defendant's Internet connection is sometimes unwittingly done by a neighbor, but has also been done by malicious third-parties wishing to avoid detection of illegal activity or to implicate a defendant in a crime. Due to the technical nature of the WFR, most users set-up the device and never touch it again unless there is a problem. Most users will never know their Internet connection was illegally used by third parties unless they receive some notification. One such common notification is the Digital Millennium Copyright Act (DMCA) take-down notice from a copyright content owner. Note: most pornography copyright content owners do not issue DMCA take-down notices to ISPs and their customers (Doe defendants). Due to the very limited network logging ability of most WFR, by the time the ISP notifies the subscriber of a legal action (such as this case), any WFR logs showing possible third-party users are long gone. If DMCA take-down notices were immediately issued to the ISPs and Doe defendants, there is a better chance of the WFR having relevant logs.

Two 2011 Federal court filings from defendants in a similar California copyright infringement case (*3:11-cv-02766-MEJ, Northern District of CA, Patrick Collins v. Does 1-*

2590, Documents 22 and 52), show how weak the Public IP address is in identifying the actual copyright infringers.

In document 22 (3:11-cv-02766-MEJ), Bobbie Thomas (ISP subscriber), Richmond, CA, tells the court she is a disabled female who lives with her adult daughter and several in-home care providers. The residence (location of the Public IP address) is a three-story building in which her daughter runs a child day care business for 12-hours a day. In the first floor common area, Mrs. Thomas' personal computer and Internet connection were open and available for any of the residents or anyone with access to use.

In document 52 (3:11-cv-02766-MEJ), Steve Buchanan (ISP subscriber), Phoenix, AZ, tells the court that unknown personnel were abusing his Internet connection and his ISP had to help him re-secure his WFR. Mr. Buchanan enlisted the help of his ISP after receiving notification from his ISP that copyright protected movies were being shared via his public IP address. Mr. Buchanan eventually secured his WFR and determined that unknown personnel had also illegally accessed his wife's computer and prevented it from connecting to his network.

The unauthorized use of a home WFR led to one Buffalo, NY, family to being investigated for allegedly downloading child pornography. On 7 March 2011, US Immigration and Customs (ICE) agents executed a search warrant for child pornography based only on the subscriber information (Public IP address) they received from the ISP. ICE later determined that a next-door neighbor had used the Internet connection via the WFR.²

In July 2011, Barry Ardolf, Minnesota, was convicted of hacking a neighbors (Matt and Bethany Kostolnik) WFR, trying to frame them with child pornography, sexual

²http://www.huffingtonpost.com/2011/04/24/insecured-wifi-child-pornography-innocent-man-accused-of-child-pornography-after-neighbor-pirates-his-wifi_24_apr11

harassment, and even sending threatening emails to Vice President Joe Biden.³ Mr. Ardolf used freely available software and manuals to hack the Wired Equivalent Privacy (WEP) protecting the Kostolnik's WFR. Due to the threatening emails sent to the Vice President, the US Secret Service contacted Mr. Kostolnik based on the email and Public IP address. Mr. Kostolnik was eventually cleared of these allegations after it was determined Mr. Ardolf hacked their WFR. Mr. Ardolf was eventually sentenced to 18 years in prison (*case 0:10-cr-00159-DWF-FLN, USDC, District of Minnesota*).⁴

Examples of why the registered IP subscriber did not illegally download/share the copyright protected movie are:

- a. Home Wireless Internet access point run open (like at an airport or coffee bar) and abused by an unknown person.
- b. Guest at the residence abusing the Internet connection without the owner knowing.
- c. Neighbor connects (knowingly or unknowingly) to the network and the owner doesn't know of this activity.
- d. IP address is part of a group residence (roommates), apartment building, or small home business where a user (not the ISP subscriber) downloaded/shared copyright protected movie.
- e. Home system infected by a Trojan Horse malware program and controlled by unknown personnel.
- f. Unknown person hacks the Wireless security settings of the WFR to abuse the owners Internet connection.⁵

Without additional investigative steps, innocent personnel are bound to be implicated in infringement activity and pressured to pay a settlement to make the threat of a federal law suit go away. One earlier court noted the problem with only using the Public IP address to identify the alleged infringer:

³<http://www.networkworld.com/news/2011/071311-wifi-hack.html>, "Depraved" Wi-Fi hacker gets 18 years in prison, 13 Jul 11.

⁴http://www.wired.com/images_blogs/threatlevel/2011/07/ardolfedssentencingmemo.pdf, Government's Position With Respect to Sentencing, 14 Jul 11.

⁵<http://www.kb.cert.org/vuls/id/723755>, WiFi Protected Setup (WPS) PIN brute force vulnerability, Vulnerability Note VU# 723755, 27 Dec 11

Comcast subscriber John Doe 1 could be an innocent parent whose internet access was abused by her minor child, while John Doe 2 might share a computer with a roommate who infringed Plaintiffs' works. John Does 3 through 203 could be thieves, just as Plaintiffs believe, inexcusably pilfering Plaintiffs' property and depriving them, and their artists, of the royalties they are rightly owed. . . . Wholesale litigation of these claims is inappropriate, at least with respect to a vast majority (if not all) of Defendants. *BMG Music v. Does 1-203*, No. Civ.A. 04-650, 2004 WL 953888, at *1 (E.D. Pa. Apr. 2, 2004) (severing lawsuit involving 203 defendants).

Without informing the court of these facts, it is irresponsible for Mr. Fiore to tell the court that ALL the defendants installed BitTorrent software and knowingly took part in the illegal download/sharing of a copyright protected movie just because Plaintiff recorded their public IP address.

9. Media Access Control (MAC) Address

The MAC address the ISPs have on record for Doe defendants is a type of serial number found on devices with a computer networking capability. Common networking enabled devices include computers, smart phones, video game systems, televisions, and DVD players. Many ISPs use the MAC address as a screening filter to limit access to their network to only the paying customers. Depending on the specific ISP, the MAC address recorded may be for the cable/DSL modem or the first network enabled device connected to the modem. If a Doe defendant only has one computer connected directly to the cable/DSL modem, then the ISP may record the MAC address for this device. As it is common today for personnel to first connect a WFR into the cable/DSL modem, the MAC address recorded by the ISP may be for this device. None of MAC addresses for the internal devices connected to the WFR (wired or wireless) are seen or recorded by the ISP or anyone else outside of the home network (Exhibit A). As previously stated, the logging ability of the WFR is very limited and the fact that Plaintiff waited so long to file this case, relevant logs are likely gone.

10. Determination of the Actual Infringer

Plaintiff has no intention of identifying the actual copyright infringers with this action. Plaintiff's goal is to obtain ISP subscriber information for the public IP addresses they recorded, issue settlement demands, and eventually dismiss the cases without naming or serving a single defendant. Plaintiff claims the public IP address shows the ISP subscriber is responsible for the infringement activity. As shown above, this logic is flawed and to truly determine the infringer, more investigative effort has to be accomplished. The history of copyright infringement law suits by pornography content owners shows the overwhelming majority of defendants are never named and served with a summons. On 24 Feb 2012, Prenda Law Inc., one of the main copyright infringement law firms in the U.S., stated the following.

Although our records indicate that we have filed suits against individual copyright infringement defendants, our records indicate no defendants have been served in the below listed cases. (*AF Holdings LLC, v. Does 1-135, case 5:11-cv-03336-LHK (NDCA), Document 43 (Declaration of Charles Piehl), Exhibit A, section 9.*)

Note: the number of cases in the Prenda document was 118, with over 15,000 Doe defendants since 2010. Out of 15,000+ Doe defendants, none were named and served with a summons (as of 24 Feb 12). I'm confident that if asked to produce a similar document, Mr. Fiore's report would be very similar for the cases he has filed in the EDPA.

11. Order & Report & Recommendation, Case 2:11-cv-03995, Judge Gary Brown (EDNY)

The basis of the 14 May 12, hearing was to address concerns the court had with Plaintiff's cases, as raised by Judge Brown's 1 May 12, Order & Report & Recommendation (ORR), Case 2:11-cv-03995, Document 39, Eastern District of New York. It is shocking Mr. Fiore didn't know about this ORR, as it deals with his client directly and was seen as a major set-back to the current copyright infringement law suits in EDNY and highly relevant to all law firms pursuing

these cases.

The court's question to Mr. Fiore about placing all of these types of copyright infringement cases under one judge is a valid one. Mr. Fiore doesn't directly state they shouldn't be placed under one judge, but he infers it is likely his view. Mr. Fiore incorrectly tells the court that as these copyright infringement cases are all "different," they should not be consolidated under the same judge. The issue is not that all of the EDPA pornography copyright infringement law suits have different Plaintiffs, different movies, and different Doe defendants. The key issue is they are all the same type of pornography copyright infringement law suit. Here are the main reasons why the EDPA should consolidate them under one judge (or limited number).

- These cases can be highly technical and a good understanding of computers/networking and Internet file sharing is needed. Having to repeatedly educate judges new to this case type on the technical aspects is a waste of limited judicial resources.
- The consolidation will ensure a uniform response for Plaintiffs and Doe defendant motions and case management, independent of which court the case is assigned to.
- All of the complaints for these cases are for Copyright Infringement in accordance with Title 17, Section 101.
- All of the alleged infringed copyright protected content is adult pornography.
- All of the alleged copyright infringement occurred via Internet file sharing applications, primarily BitTorrent.
- All the Plaintiffs in these cases employ some sort of technical monitoring service to record the public IP address of alleged infringers.
- All cases deal with Doe defendants who are only identified by their public IP address.

- All Plaintiffs seek leave to serve third party subpoenas prior to a Rule 26(f) Conference. The third party is the ISP who has the contact information (name, address, telephone number, email) for the subscriber assigned the public IP address Plaintiff recorded.
- Many Doe defendants in these cases file motions to quash, dismiss, or sever, based on claims of improper joinder, improper jurisdiction, or lack of prima facie evidence.
- Once the contact information for the Doe defendants are obtained, Plaintiffs make settlement demands of thousands of dollars to make the fear of a law suit go away.
- For over 200,000 Doe defendants nation-wide since 2010, there have only been a handful of default judgments issued. Most Plaintiffs dismiss the cases against non-settling Doe defendants. The goal with these types of law suits is not to prevent copyright infringement, but to generate revenue on a repeatable basis.

In his ORR (case 2:11-cv-03995), Judge Brown correctly described the litigation practices of these cases as "Abusive."

Our federal court system provides litigants with some of the finest tools available to assist in resolving disputes; the courts should not, however, permit those tools to be used as a bludgeon. As one court advised Patrick Collins Inc. in an earlier case, "while the courts favor settlements, filing one mass action in order to identify hundreds of doe defendants through pre-service discovery and facilitate mass settlement, is not what the joinder rules were established for." *Patrick Collins, Inc. v. Does 1-3757*, 2011 U.S. Dist. LEXIS 128029, at *6-7 (N.D.Cal. Nov. 4, 2011).

After my personal information was released to my Plaintiff, I was repeatedly threatened with an individual law suit. I was told I was responsible and there was no defense. I was told that unless I settled, the case would drag on for a year or two, and it

would cost me thousands more dollars than settling. My Plaintiff eventually dismissed the case after keeping it open for more than a year. I was never named in any complaint and never received a summons, even after repeated calls and letters stating they were about to take such actions. On 1 December 2011, Judge Maria-Elena James, Northern District of California (*case # 3:11-cv-02766-MEJ, Patrick Collins v. Does 1-2590*), commented on this practice.

Since granting Plaintiff's request, a check of the Court's docket disclosed that no defendant has appeared and no proof of service has been filed. Further, the Court is aware that this case is but one of the many "mass copyright" cases to hit the dockets of federal district courts across the country in recent months. Like in this case, after filing the suit, the plaintiff seeks discovery from ISPs who possess subscriber information associated with each IP address. With the subscriber information in hand, the court is told, the plaintiff can proceed to name the defendants in the conventional manner and serve each defendant, so that the case may proceed to disposition. This disposition might take the form of settlement, summary judgment, or if necessary, trial. In most, if not all, of these cases, if the plaintiff is permitted the requested discovery, none of the Doe defendants are subsequently named in the cases; instead, the plaintiff's counsel sends settlement demand letters and the defendants are subsequently dismissed either by the Court or voluntarily by the plaintiff.

12. Conclusion

The copyright infringement of protected works, such as Plaintiff's, is a problem and the owners have the right to seek redress for it. Plaintiff's misuse of the court in seeking redress stems from the weak prima facie evidence collected (public IP address) coupled with abusive settlement practices. Plaintiffs commonly set the settlement fee for defendants at the point where it costs them more to fight than settle, regardless of guilt or innocence. The threat of possible financial ruin, family and friend embarrassment, a convenient settlement option, and non-disclosure agreement, make it easy for even innocent people to possibly accept paying the settlement fee. Plaintiff knows their evidence collections methods are not 100% effective at identifying the actual infringers. To admit this short coming risks the prof-

itability of this business model and future operations. The fact that a majority of Federal civil cases are settled before trial should not be the justification basis for allowing this activity to continue. Plaintiff and the growing number of copyright infringement lawyers are abusing the court for their financial gain. These cases and other like it in the EDPA (past, present, and future) will follow the standard course of action: (1) release of ISP subscriber information, (2) settlement demands made by Plaintiff, and (3) dismissal of the cases after settlements are collected from some defendants (Noting that no defendants will be named and served).

I thank the court for hearing this declaration.

Dated: 5/31/2012

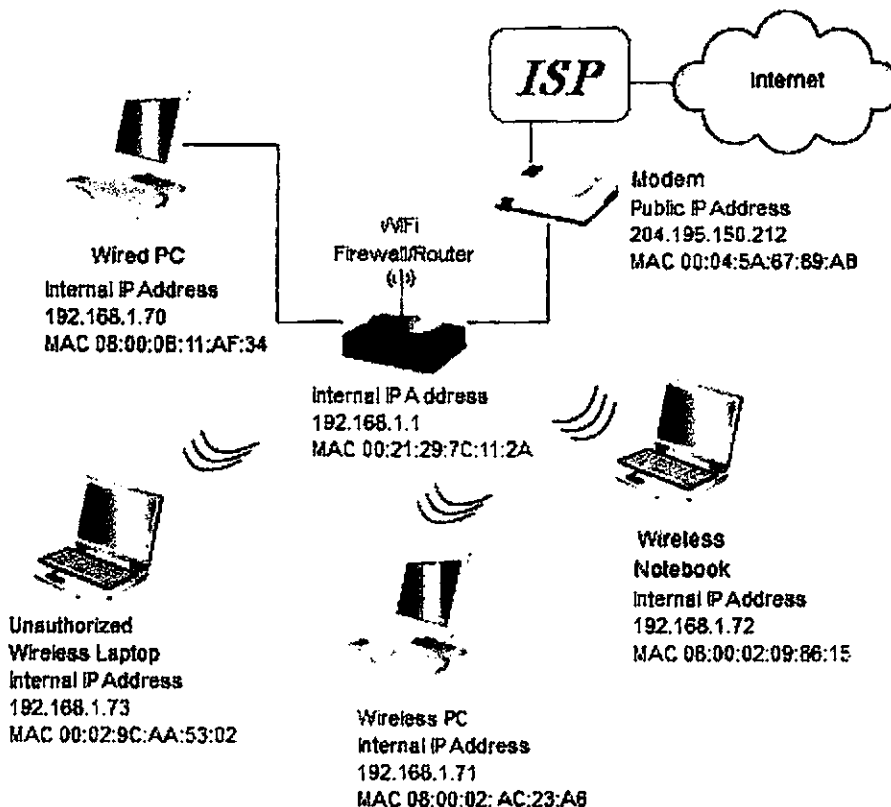
Respectfully submitted,



John Doe, AKA: DieTrollDie
Web site: <http://dietrolldie.com>
Doerayme2011@hotmail.com

EXHIBIT A (2:12-CV-02084)

Example of home network using a Wireless Firewall/Router



The following table is an example of a Dynamic Host Configuration Protocol (DHCP) host table maintained inside the Wireless Firewall Router. It shows the names, Internal IP address, MAC addresses, and IP address lease expiration time for systems that are connected to the network.

Note: this example does not directly correspond to the network diagram above.

DHCP Active IP Table

DHCP Server IP Address: 192.168.1.1

Client Host Name	IP Address	MAC Address	Expires	
SpuraSPA	192.168.1.84	00:0E:08:CD:C9:98	20:01:49	<input type="checkbox"/>
stephani-15adea	192.168.1.85	00:0C:76:68:C4:0A	08:49:53	<input type="checkbox"/>
admin-krori9y18	192.168.1.86	00:98:02:FE:BB:22	23:43:47	<input type="checkbox"/>
luca-ba6m1f9a	192.168.1.89	00:20:ED:33:70:F4	13:12:54	<input type="checkbox"/>

Refresh

Delete

Close

CERTIFICATE OF SERVICE

I hereby certify that on 5/31/2012, I served a copy of the foregoing document, via US Mail, on:

Fiore & Barber LLC
Attn. Christopher Fiore
425 Main Street, Ste 200
Harleysville, PA 19438

Dated: 5/31/2012

Respectfully submitted,

John Doe

John Doe, AKA: DieTrollDie
Web site: <http://dietrolldie.com>
Doerayme2011@hotmail.com

Exhibit B

Part 1

District of Columbia

THIRD DEGREE FILMS, INC.
20525 Nordhoff Street, Suite 25
Chatsworth CA 91311

v.

Does 1-152

DECLARATION OF STEPHEN HENDRICKS

Case CA 1:11-CV-01833-BAH

Judge Beryl Howell

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

THIRD DEGREE FILMS, INC.)	
20525 Nordhoff Street, Suite 25)	
Chatsworth CA 91311,)	
)	
Plaintiff,)	
)	
v.)	CA 1:11-CV-01833-BAH
)	
DOES 1-152,)	
)	
Defendants.)	

DECLARATION OF STEPHEN HENDRICKS

My name is Stephen Walker Hendricks. I am an Advanced Systems Representative Tier 1 and Tier 2 (Tier 2 is obsolete but still my title) at Comcast Cablevision based in Whitmarsh, Maryland. I have been a micro computer builder, designer and support technician since 1980 having been employed also at Heath Zenith Computers in Towson, MD from 1986 to 1989 as a sales agent who also custom built, and maintained systems for government, business, and individual clients. In my job capacities it was my responsibility to assist clients in all manners of computer operations, including helping using to protect their computers from threats which included viruses, malicious software, hardware vulnerability as well as human threats.

I have been provided the Complaint and its exhibits in the case of *Third Degree Films, Inc. v. Does 1-152*, Case No: 1:11-cv-01833-BAH.

The Declaration of Jon Nicolini, Exhibit B to the Complaint, contains misleading and erroneous statements that must be corrected.

1. It is impossible for Comcast to determine what devices attained the IP addresses

attributed in Exhibit A to John Does 116 and 117. IP addresses are dynamically assigned using the Dynamic Host Configuration Program (DHCP) protocol. The use of dynamically assigned IP addresses means that any device that is connected to a Comcast Cable modem can have different IP addresses based on several different events. An IP address can be used by several different devices simultaneously on the local network (referred to as a subnet) with the use of malicious programming techniques which can obscure the origin of an actual computer's connection. A subnet may have a few IP addresses in use, or hundreds of IP addresses. An ISP connects to the Internet through a direct connection.

2. The main computers which establish this connection are in an office called the Head End. The computers which connect the end user's computer (or other device) to the Internet are referred to as the Head End Computers. The Head End Computers communicate with devices that are attached to its fiber optic and coaxial cable systems using a standard referred to as Data Over Cable Service Interface Specification (DOCSIS). DOCSIS devices include modems and cable television set top boxes, televisions, and other devices. These devices also connect to the Head End using Ethernet data protocol and appear to the local network as computer devices. Television, cable boxes, disc players, and other devices now commonly used in a home can all communicate using IP protocol.
3. The only criterion that a computer Ethernet device needs to establish a connection to a DOCSIS cable modem is that it must use a connection protocol (in ISPs like Comcast the protocol is DHCP) and that it must provide to the modem a hardware

address called a MAC address. A modem can provide a connection to the Internet which will give the device connected to the Internet an IP address. The ISP however, cannot determine any of the following:

- a. Whether the device using the Internet connection is a computer, mobile device, tablet, router, etc.
 - b. The precise location of the device, since the modem can be anywhere on a subnet
 - c. How many devices may be using a particular IP address to access the Internet
 - d. If the MAC address is a true MAC address representing the Ethernet device or one that is spoofed (copied and reused) by some other device (such as an Ethernet connection on a Linux computer system, or a router).
4. A specified IP address cannot be assumed to belong to any particular device since the hardware address of a device can be spoofed.
 5. It is not possible to say what devices were connected to Ms. Zwarycz's Comcast Internet connection, by whom they were being used, and where the devices were physically located at the time they being used (i.e., inside the house of Bailey Zwarycz, in a neighboring house, or in a vehicle parked outside the Zwarycz residence or in a nearby structure which has access by cable to the same subnet).
 6. In fact, it is impossible for anyone to determine what device negotiated the IP addresses attributed in Exhibit A to John Does 116 and 117.
 7. Knowing an IP address that was being provided to a cable modem connection

does not identify the device that is connected through that modem. Even if the copyrighted material in question was being delivered over the Internet through that IP address there is no way to know or prove where it originated or that the owner of the Internet connection with that IP address, if she owns a computer, ever hosted or was the source of said material. The material may have come from:

- a. Any device connected to the local subnet accessing the Internet through Ms. Zwarycz's Internet connection.
 - b. An external wireless connection.
 - c. An external relay through a remote control virus.
 - d. A smart phone, tablet, laptop, or even surreptitious access of the subscriber's computer gained by a computer hacker without Ms. Zwarycz's knowledge.
8. For the reasons stated above, it is false and baseless for the Nicolini Declaration to say that by knowing the IP addresses of John Doe 116 and 117 they could determine whether a computer had been used and if so, which computer. (See Jon Nicolini Declaration, Complaint Exh. B, Paragraphs 18-21.)
9. Even if an unknown person downloaded Plaintiff's film using the IP address Comcast associates with Ms. Zwarycz, that person could have been using a computer outside of the house of Ms. Zwarycz without her awareness, knowledge, or consent.

10. The primary upshot of the foregoing information for this case is that there is no way that Plaintiff could make a good faith allegation in its complaint that John Does 116 and 117 -- namely, Bailey Zwarycz-- willfully and intentionally downloaded, copied, and distributed Plaintiff's film. (See Jon Nicolini Declaration, Exhibit B to Complaint, Paragraphs 18-21.)

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on January 29, 2012.

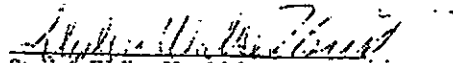

Stephen Walker Hendricks

Exhibit B

Part 2

District of Columbia

THIRD DEGREE FILMS, INC.
20525 Nordhoff Street, Suite 25
Chatsworth CA 91311

v.

Does 1-152

DECLARATION OF SENSEI ENTERPRISES, INC.

Case CA 1:11-CV-01833-BAH

Judge Beryl Howell

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Third Degree Films, Inc.,
Plaintiff,
v.
Does 1 - 152,
Defendants.

**DECLARATION OF
SENSEI ENTERPRISES, INC.**

**Case No: 1:11-CV-01833-BAH
Judge Beryl Howell**

I, John W. Simek, declare as follows:

1. I am the Vice President of Sensei Enterprises, Inc. and have been so employed as such since January of 1997.
2. Sensei Enterprises is an information technology, information security and computer forensic company located at 3975 University Drive, Suite 225, Fairfax, VA 22030.
3. Sensei Enterprises has been retained to review documents and devices in connection with the matter of *Third Degree Films, Inc. v. Does 1-152*, specifically the following:
 - a. The Complaint and its Verification by Mike Meior, an attorney located at 4000 Legato Road, Suite 1100, Fairfax VA 22033- executed under the provisions of 28 USC Section 1746.
 - b. A Declaration filed in this action and prepared and executed by Jon Nicolini, Vice-President of Technology for Copyright Enforcement Group, LLC, of Beverly Hills California, executed under the penalty of perjury and stated to be of his personal knowledge.

- c. The Declaration of Bailey Zwarycz.
 - d. The laptop computer owned by the person identified in the Complaint as John Doe 116 and 117.
4. I disagree with numerous factual recitations and the conclusions drawn from those recitations by Messrs, Meier and Nicolini as set forth in the Complaint and the Declaration of Mr. Nicolini. The disagreements and the basis for the disagreements are as follows:
- a. The Complaint asserts, and Messrs, Meier and Nicolini endorse the assertions as factually accurate and truthful, that once the Plaintiff is provided the subscriber identity from the Internet Service Provider (ISP) as determined from the Internet Protocol (IP) address, that they will have learned the actual identity of the person or persons alleged to have willfully and intentionally downloaded the copyright protected film, otherwise known as "All About Kagney Linn Carter," an admitted pornography film. The IP addresses are identified in Exhibit A of the Complaint. Messrs, Meier and Nicolini misrepresent the conclusions as fact when only the IP address is known. The public IP addresses as identified in Exhibit A only represent the last identifiable hardware device that is connected to the Internet, through which the Plaintiff's copyrighted material may have passed on its way to a destination or destinations unknown.
 - b. The two IP addresses listed for John Doe 116 and John Doe 117 are associated with the same single physical device associated to a single subscriber. John Doe 116 and John Doe 117 are the same person, for which two unique dynamic IP addresses were assigned by the John Doc's Internet Service Provider.

- c. John Doe 116 and John Doe 117 shall hereinafter be referred to in the singular as "this John Doe."
- d. The device assigned the two IP addresses is passed through a cable modem, which is used to connect subscriber equipment to the ISP's network. The cable modem converts the signal of the ISP network to a format that is compatible with other network attached devices of the subscriber. This may include such items as a single computer, network switch or router. The cable modem itself does not record or store the transmitted information, but is merely a pass-through device changing one signal type to another for use by digital devices at each end. In no sense are they capable of downloading and storing the Plaintiff's protected material or applying any software to that signal to act as a "seed" or a "swarm" as described by the Complaint and the declarations of Meier and Nicolini.
- e. It is well known that the majority of users accessing the Internet via a broadband (e.g. cable modem, DSL, etc.) connection do so by using a router, which is a device that attaches to the cable modem or similar equipment and allows multiple users to access the Internet simultaneously through a single connection. Routers, like cable modems, are not in and of themselves capable of downloading, storing, recording, or manipulating data such as the Plaintiff's protected material. The presence of a router connected to the cable modem obtains the IP address assigned by the ISP and appears as if it is a single computer to the ISP.
- f. This John Doe's Internet service provider was Comcast and the cable modem used to connect this John Doe's computer to the Internet was also provided by Comcast, which maintained a record of the modem's Media Access Control

(MAC) address associated with it. The MAC address can be thought of as a hardware serial number for the device.

- g. This John Doe had acquired a wireless router independently of Comcast and the presence or absence of a router attached to her cable modem was not known or knowable to Comcast. Comcast only knows that *some* device is attached and presents itself as having a specific IP address.
- h. Routers may be "password protected" so that they theoretically can only be accessed by users who have knowledge of the correct password. In addition, the wireless "cloud" can also be password protected to prevent unauthorized access.
- i. Router owners, such as this John Doe, may grant as many people as they choose to access the Internet through their router [up to certain finite limits not relevant here].
- j. This John Doe can elect to use a wireless router which is not protected by a password, thus enabling anyone within the wireless signal range of the router to access the Internet through this device.
- k. Even if the wireless "cloud" was password protected there are several commercially available (and free) programs able to determine the wireless password and circumvent it.
- l. So long as the last identifiable device in the chain of distribution is a cable modem (known via MAC address), to which a wireless router may be attached, the ultimate user who accessed the Internet and downloaded some or all of the Plaintiff's protected material and used peer-to-peer network software to acquire,

assemble and redistribute its protected material may be unknown and indeterminable.

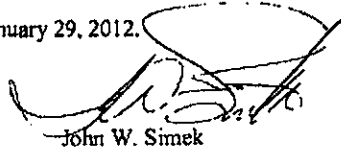
- m. Absent special software or hardware acquired for that purpose, knowing how many users may be accessing the Internet simultaneously through the same wireless router is not apparent to any person or persons utilizing the wireless router.
- n. I have been advised that this John Doe is a student at Virginia Polytechnic University (Virginia Tech) who attached an un-password-protected wireless router, which she obtained commercially, to her Comcast provided cable modem. At the time she did so she was unaware that the wireless "cloud" was not protected by a password and even unaware that the wireless "cloud" could be secured via a password.
- o. I have been advised that this John Doe accessed the Internet through the use of a laptop computer which connected wirelessly to her router. She has a vague memory of occasions when others who visited her in her quarters may have accessed the Internet wirelessly through her router. She was completely unaware that others outside her dwelling place might have access to the Internet through her router with or without her permission or knowledge.
- p. On the 2nd day of December, 2011, at the request of counsel, Sensei took delivery of her laptop computer, forensically acquired her entire hard drive and thereafter returned the laptop to her. We then conducted an examination of the contents of that hard drive, using professionally accepted techniques and tools, looking for any indication that at any time the laptop had downloaded, stored or manipulated

any portion or all of the Plaintiff's protected material, or had on its hard drive any software capable of participating in a peer-to-peer network, specifically for any part or all of a programs capable of participating in a BitTorrent network.

- q. The techniques and tools used would have uncovered any indicia of the downloading, storing or manipulation of the Plaintiff's protected material currently on the computer system, and even if that material had once been present but was subsequently deleted or uninstalled, remnant data or artifacts of such data would most likely still be present.
 - r. The same professionally accepted techniques and tools were used to search for any indicia of the past or present use of peer-to-peer software or the BitTorrent network. No evidence was discovered of such usage or presence of software to facilitate usage.
 - s. It is my professional judgment that at no time in the past or in the present has the hard drive of this John Doe's computer contained any part of the Plaintiff's movie "All About Kagney Linn Karter" or any part of peer-to-peer software or BitTorrent network access. I hold this opinion with a high degree of confidence, that is, to a reasonable degree of scientific certainty.
5. In the Meier verified Complaint and the Declaration of Jon Nicolini they further contend that they were able to determine that all of the John Does, including John Does 116 and 117 were within the jurisdiction of this court, contending they used "geo-location technology..." to attempt to "ensure that the IP Addresses are likely within the geographic location of the Court."

- a. Mr. Meier specifically asserts that he “personally spot checked the purported location of the alleged infringers...” using “the IP locator at <http://www.ipligence.com>.”
 - b. According to the Declaration of this John Doe, the location of the wireless router connect to the Comcast cable modem represented by those two listed IP addresses for John Doe 116 and 117 is and always has been in Blacksburg, Virginia.
 - c. When I used the website (<http://www.ipligence.com>) specified by Mr. Meier to determine the probable location of the IP addresses stated for John Does 116 and 117, it returned Richmond, Virginia and an unknown city in Missouri. Obviously, both locations are inaccurate as the subscriber is located in Blacksburg, Virginia.
 - d. I used several other geolocation websites and the location for the IP addresses for John Doe 116 and 117 always returned a location of Blacksburg, Virginia.
6. Plaintiff acknowledges that it does not know the identity of this John Doe. Armed only with the IP address of this John Doe’s device attached to the cable modem, it was impossible for Plaintiff to be able to ascertain the actual identity of this John Doe or that this John Doe “willfully and intentionally downloaded, copied, and distributed” the film in question or any other film.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on January 29, 2012.



John W. Simek