

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLORADO**

Civil Action No. 12-cv-01873-RBJ-MEH

MALIBU MEDIA, LLC,

Plaintiff,

v.

LINDSEY MANESS,

Defendant.

---

**DEFENDANT’S MOTION TO DISMISS PLAINTIFF’S COMPLAINT FOR FAILURE  
STATE A CLAIM**

---

Defendant, Lindsey Maness (“Defendant”), by and through undersigned counsel and pursuant to Fed.R.Civ.P. 12(b)(6), 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 “[a]s the subscriber of the internet service being used to distribute Plaintiff’s copyrighted movies, Defendant is the *most likely* infringer.” (Complaint ¶23)(emphasis added). This conclusion is prefaced exclusively on a boilerplate declaration executed by the employee of “a company

organized and existing under the laws of Germany.” (Complaint, Exhibit C at ¶4) (hereinafter “the Feiser Declaration”.) The Feiser Declaration, however, provides no information or details whatsoever as to how 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 Feiser Declaration provided to support Plaintiff’s already thread-bare claims, as will be discussed below, is factually inaccurate and misleading. Neither the Feiser Declaration nor Plaintiff’s Complaint 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.”)).

Perhaps more troubling is the fact that Defendant has repeatedly offered the Plaintiff near “unfettered access” to his computers and network and copies of documentary and other affidavit evidence demonstrating a full preservation of evidence as well as his innocence, yet he still finds himself pressured to settle for thousands of dollars, or face the task of mounting a expensive and time-consuming defense.<sup>12</sup>

---

<sup>1</sup> Defendant advised counsel that he has never downloaded, uploaded or traded any movies through the internet, and did not even know what BitTorrent was until contacted by Plaintiff’s “settlement representatives,” nor is he aware of anyone that might have downloaded the works, if such an event even occurred and will execute a declaration to that effect. Defendant also has documentary evidence that other family members in his home were not even physically present during some of the alleged downloading dates, and that at times his wireless router was unprotected. Defendant also has evidence that near in time to the alleged “hit dates” his computer was the victim of a hacker/virus necessitating the purchase of an entirely new operating system. In the end, Defendant chose not to submit this evidence because he did not want to introduce unnecessary confusion into the instant Rule 12(b)(6) motion, which examines solely the legal sufficiency and plausibility of the Plaintiff’s allegations.

<sup>2</sup> 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 litigations 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 “farical.” *Id.* at n7. More on point, the Court identified the exact scenario with which the Defendant is presented with, namely offering unfettered access to their networks and computers coupled with affidavit evidence of innocence and the preservation of evidence. *C.f. Id.* at 28. (“In this case, John Doe #16 offered the Plaintiff “unfettered access” to his computer and employment records demonstrating that he was not at home at the time of the downloading.”). (*See also* Affidavit of Christina Saunders; David S. Kerr; and John Arsenault as Exhibits A.)

## 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 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)).

---

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.

## 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 copyright<sup>3</sup> 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 “Defendant is the most likely infringer.” (Complaint ¶23) Furthermore, Plaintiff’s already threadbare Complaint is only supported by a single boilerplate Declaration that is both factually inaccurate and misleading.

#### 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 most likely infringer” is a guess. (Complaint ¶23). 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 was identified by his Internet Service Provider (“ISP”) as the subscriber for internet service that was allegedly

---

<sup>3</sup> Defendant specifically reserves the right to contest not only validity but ownership of such copyright(s) at a later date.

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 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.”).

Even this Court 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 ¶23). 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 failed to carry this burden and its Complaint should be dismissed.



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 Defendant is the “*most likely infringer*” meaning that he 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 DECLARATION 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 Defendant is the “most likely infringer.” (Complaint ¶23.) As noted above, these claims find sole support in a boilerplate declaration that does not specifically identify the Defendant, the Defendant’s Internet Service Provider (“ISP”), or even the IP address at issue.<sup>4</sup> While it generally describes the procedure for collecting IP addresses, the Feiser Declaration includes no assertion that such steps were taken in this matter. (Feiser Declaration at ¶22.) For example, despite acknowledging that “ISPs keep track of the IP addresses assigned to their subscribers” the Feiser Declaration does not state that any ISP was ever contacted regarding this matter. In short, the Feiser Declaration 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. In addition, and perhaps more fatal to Plaintiff’s allegations, the Feiser Declaration 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 Feiser Declaration states that an “IP address is a unique numerical identifier that is automatically assigned to an internet user by the user’s Internet Service Provider (“ISP”).

---

<sup>4</sup> 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 Mr. Feiser’s entire 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).

(Feiser Decl. ¶7). 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 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. The Feiser Declaration contradicts itself later conceding that that the ISP can only correlate an IP address to “the subscriber of the internet service.” (Feiser Declaration ¶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 Feiser Declaration’s statement that the information listed in Exhibits A and B of the Complaint identified the “infringement committed by the Defendant in this case.” (Feiser Decl. ¶18). The Feiser Declaration goes onto to make the unsupported statement that a “computer using the IP address assigned to Defendant” participated in the alleged infringing activity, (*Id.* at ¶19), and that the ISP can “identity the name...of the Defendant.” (*Id.* at ¶22). 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 Mr. Feiser or 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 Mr. Feiser’s, 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 ¶6).<sup>5</sup> Such inaccurate and misleading evidence offered in bad faith cannot support Plaintiff’s claims and its Complaint should be dismissed.

Third, the Feiser Declaration’s conclusory and unsupported statements 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;<sup>6</sup>
2. A client requesting a download can substitute another IP address for its own to a Bittorrent tracker;<sup>7</sup>

---

<sup>5</sup> Similar to the Defendant referenced in both the Hendricks and Simek declarations, Defendant’s ISP is Comcast.

<sup>6</sup> 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.”).

<sup>7</sup> 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/uwse\\_dmca\\_tr.pdf](http://dmca.cs.washington.edu/uwse_dmca_tr.pdf) See also, “IP address spoofing” [http://en.wikipedia.org/wiki/IP\\_address\\_spoofing](http://en.wikipedia.org/wiki/IP_address_spoofing) (Last visited August 2, 2012) (the term IP

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;<sup>8</sup>
4. Malware on a computer can host and distribute copyrighted content without knowledge or consent;<sup>9</sup>
5. There are reliability issues with using IP addresses and timestamps to identify the correct party;<sup>10</sup>
6. If a subscriber has dynamic IP addressing through its website host, it is sharing an IP address with several other subscribers;<sup>11</sup>
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;<sup>12</sup> 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.

---

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.

<sup>8</sup> Ibid.

<sup>9</sup> Ibid.

<sup>10</sup> 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 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.")

<sup>11</sup> "Web hosting service" [http://en.wikipedia.org/wiki/Web\\_hosting\\_service](http://en.wikipedia.org/wiki/Web_hosting_service) (Last visited August 2, 2012).

<sup>12</sup> 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\\_science-wireless/](http://www.msnbc.msn.com/id/42740201/ns/technology_and_science-wireless/)

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 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 its valid copyrights 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.*<sup>13</sup>

Such admissions provide further support that Plaintiff's unsupported “guess” that Defendant is the “most likely 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, ¶¶ 23, 24); 2) 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 “most likely infringer” is likely not even supportable under Fed.R.Civ.P. 11, let alone

---

<sup>13</sup> These aforementioned admissions may be judicially noticed by this Court. See generally *St. Louis Baptist Temple v. FDIC*, 605 F. 2d 1169, 1171-1172 (10<sup>th</sup> 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.”).

Fed.R.Civ.P. 12(b)(6).<sup>14</sup> 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 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).

---

<sup>14</sup> Counsel for Defendant has been authorized to evaluate the possibility of seeking sanctions under Rule 11 and other bases and will proceed appropriately.

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 Defendant -- 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.

### **III. CONCLUSION**

Plaintiff's allegations against Defendant in this case are premised on the mere possibility that he 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 October 17<sup>th</sup>, 2012.

SANTANGELO LAW OFFICES, P.C.

/s/ David S. Kerr  
David S. Kerr  
125 South Howes St., 3rd Floor  
Fort Collins, CO 80521  
Telephone: 970-224-3100  
Email: dkerr@idea-asset.com

**CERTIFICATE OF COMPLIANCE WITH D.C.COLO.LCIVR 7.1**

Pursuant to D.C.Colo.L.CivR. 7.1(A), counsel for Mr. Maness has conferred with Plaintiff's counsel in compliance with the aforementioned rule.

**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 EFS and email on this 17<sup>th</sup> day of October, 2012 upon the following counsel:

Jason Kotzker  
Kotzker Law Group  
9609 S University Blvd., #632134  
Highlands Ranch, CO 80163  
[jason@klgip.com](mailto:jason@klgip.com)

/s/ David S. Kerr  
Santangelo Law Offices, P.C.  
125 South Howes St., 3rd Floor  
Fort Collins, CO 80521  
Facsimile: 970-224-3175  
Telephone: 970-224-3100  
Email: [dkerr@idea-asset.com](mailto:dkerr@idea-asset.com)