

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

FILED
U.S. DISTRICT COURT
DISTRICT OF COLORADO
2012 OCT 11 PM 1:23
JEFFREY B. COLWELL
CLERK
BY _____ DEP. CLK

Civil Action No. 1:12-cv-02069-WYD-MEH

MALIBU MEDIA, LLC.

Plaintiff,

v.

Does 1-31,

Defendants.

**MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANT
JOHN DOE #4'S MOTION TO QUASH THE PLAINTIFF'S SUBPOENA**

Defendant, John Doe No. 4 ("Defendant") identified at internet protocol ("IP") address 24.8.144.246 on June 10, 2012 at 19:17 UTC, respectfully submits this Memorandum of Points and Authorities in Support of Defendant's Motion to Quash Plaintiff's Subpoena served upon Defendant's Internet Service Provider ("ISP"), Comcast on August 9, 2012.

FACTUAL BACKGROUND

1. On August 9, 2012, this Court issued an Order permitting Plaintiff to serve a Rule 45 subpoena on each Defendant's internet service provider seeking personally identifying information about each Defendant, including Defendant's name, physical address, telephone number, e-mail address, and media access control ("MAC") address.
2. On August 9, 2012, Defendant's ISP, Comcast was served with a subpoena issued from this Court and served in Denver, Colorado, that demanded Comcast to produce to Plaintiff at

Plaintiff's counsel's office in Colorado, the personally identifying information regarding Defendant in connection with Plaintiff's claim that Defendant allegedly unlawfully downloaded a film allegedly owned by Plaintiffs ("work").

3. Comcast provided written notice to Defendant on August 12, 2012 via UPS delivery.
4. Comcast's August 12, 2012 letter stated that Comcast would provide the requested information to Plaintiff by September 21, 2012. Comcast's letter further advised Defendant that if Defendant had any objections to the subpoena, Defendant needed to file those objections with the Court prior to September 21, 2012.
5. United States Magistrate Judge, Michael E. Hegarty, issued a Minute Order denying without prejudice on September 27, 2012 Defendant John Doe #4's Motion to Dismiss and/or Sever Complaint Against Defendant and Quash the Subpoena Against the Same [filed September 19, 2012; docket #13] for failure to comply with Fed. R. Civ. P. 11(a) and granted Defendant until October 11, 2012 the opportunity to re-file his motion according to the Minute Order.

INTRODUCTION

I, John Doe No. 4, respectfully submit to the Court a motion to quash the subpoena served on my Internet Service Provider, Comcast Corporation.

I have never committed the acts alleged by the plaintiffs. After receiving a letter from Comcast Corporation advising me that it had been subpoenaed to release my identity and contact information in this matter, I began to research Malibu Media, LLC and similar cases brought by others. My internet research has revealed that in cases associated with Malibu Media, LLC, when the subpoenaed information is turned over to the plaintiffs, the defendants, guilty or innocent, receive demand letters. These letters typically demand from \$2500 to \$7500 and in

some cases in excess of \$15000 for settlement to avoid dealing with threatened lawsuits, and the subsequent telephone calls, which have been reported as persistent if not harassing, are the reason I am filing this motion. I respectfully request that I be allowed to make this motion anonymously without revealing my personally identifying information as to do otherwise would defeat the purpose of this motion.

The present case is one of several efforts by certain media organizations to establish a business model that relies on questionable allegations of copyright infringement against a large number of individuals to generate substantial profits by extracting settlements from thousands of identified Defendants. These actions are part of a nationwide blizzard of civil actions brought by purveyors of pornographic films alleging copyright infringement by individuals utilizing a computer protocol known as BitTorrent. Given the sensitive nature of certain adult materials and public association therefrom, Defendants are often quick to settle to avoid being named or associated with a lawsuit having to do with adult content. Federal Courts have expressed skepticism toward this business model, including this quote from the Chief Justice of the U.S. District Court for the District of Nevada about Plaintiff's "attempt[] to create a cottage industry of filing copyright claims, making large claims for damages and then settling claims for pennies on the dollar." *Righthaven, L.L.C. v. Democratic Underground*, No. 2:11-cv-01356 (D. Nev. Apr. 14, 2011), Dkt 94. Other Courts have been less generous, questioning "Plaintiffs who file cases with extremely weak infringement positions in order to settle for less than the cost of defense and have no intention of taking a case to trial. Such a practice is an abuse of the judicial system and threatens the integrity of and respect for the courts." Mem. Op. and Order at 5, *Raylon, L.L.C. v. E.Z. Tag Corp.*, No. 6:09-cv-00357 (E.D. Tex. Mar. 9, 2011), Dkt. 115.

In direct reference to Plaintiff's business model and questionable claims of copyright

infringement, Judge Beeler of the U.S. District Court for the Northern District of California, found in regards to Plaintiff Patrick Collins Inc. in a similar Bit Torrent copyright litigation case involving one-hundred-eighty-eight (188) John Doe Defendants and an order to show cause:

[t]he court has no confidence that Plaintiff has been diligent in moving to name and serve Defendants, despite its (unsworn) claims to the contrary. For example, Plaintiff's counsel states that he has filed ten other copyright cases involving a large number of Doe Defendants. ECF No. 17 at 4. The court reviewed the dockets and noted that the Plaintiffs in these cases have not filed proof of service for even a single Defendant even though a number of Defendants have been identified and dismissed after settling with the Plaintiffs. See, e.g., *Media Products, Inc. DBA Devil's Film v. Does 1-1257*, Case No. cv 10-04471 RS (complaint filed on October 4, 2010 and no proof of service filed for any Defendant as of July 29, 2011, but four Doe Defendants have been dismissed after settling). This pattern holds true in this case too. Here, Plaintiff has not identified or served any of the 1,219 Doe Defendants. However, on May 10, 2011, Plaintiff filed a stipulation dismissing with prejudice a Doe Defendant who settled with Plaintiff. ECF No. 13 at 1. And, on August 18, 2011, Plaintiff filed a stipulation dismissing with prejudice more than thirty Doe Defendants who settled. ECF No. at 1-2. The plaintiffs in these cases appear content to force settlements without incurring any of the burdens involved in proving their cases. And, 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." *IO Group, Inc. v. Does 1-435*, No. C 10-4382 SI, 2011 WL 445043, at*6 (N.D. Cal. Feb. 3, 2011).

Order Dismiss Comp. *Patrick Collins, Inc. v. Does 1-1,219*, Case 4:10-cv-004468-LB Dkt. No.27 (D. Cal. 2011) Aug. 29, 2011.

Based on the extraordinarily large number of analogous cases, treated in the same or similar manner by Plaintiffs, it appears that such mass copyright litigation lawsuits are a means "to identify hundreds of Doe Defendants through pre-service discovery," then, regardless of any consideration of guilt or innocence seek to coerce largely contingent-fee settlements, sometime through harassing letters and direct phone calls with no real intent to actually litigate such claims. This for-profit business model becomes more obvious when one considers the actual number of Defendants claimed in such action versus the astonishingly low number of actions

actually commenced.¹

Plaintiff again seeks to take advantage of the threat of an award of statutory damages, attorneys' fees, ignorance about copyright law, and the stigma associated with accessing pornography via the internet to extract quick and profitable settlements. This Court has specifically and directly condemned for-profit copyright litigation models against individuals. *Righthaven, L.L.C. v. Hill*, No. 1:11-cv-00211 (D. Colo. Apr. 7, 2011) (J. Kane), Dkt. 16 (“Plaintiff’s wishes to the contrary, the courts are not merely tools for encouraging and exacting settlements from Defendants cowed by the potential costs of litigation and liability.”) Although Plaintiff does not rely on the same business model as the Righthaven model, Plaintiff does seek to exact settlements from numerous Defendants sued in a John Doe capacity in an amount to which mounting a defense in Court is less economically efficient than settling out of court.

In light of the aforementioned authority, in its following argument, Defendant requests that the Court quash Plaintiff’s subpoena.

Moreover, because of the scandalous subject matter involved, the unique procedural posture of so many misjoined Defendants, identical cases now pending before the Court, and massive potential liabilities, that-if Plaintiff’s joint and several liability theories are to be credibly believed could result in excess of several million dollars based solely on questionable allegations of what can only be described at best as *de minimis* acts – the need to cautiously evaluate the various substantive and procedural safeguards is paramount.

Unfortunately, as has been demonstrated in similar actions around the country, some Plaintiffs in mass-copyright infringement lawsuits have at times failed to regard substantive and

¹ As of March, 2011, more than 136,000 Does claimed as Defendants in such actions, however, the number of actual copyright infringement actions commenced was less than 100. Wired Magazine’s online spreadsheet prepared from existing court data: http://www.wired.com/images_blogs/threatlevel/2011/03/spreadsheet-fslit-current-v-1.2.01.xls

procedural safeguards implemented as Federal law to protect potential Defendants. The present case is no different because Plaintiff has misjoined all thirty-one (31) Defendants to avoid the cost of appropriately filing individual cases against each John Doe Defendant.

Plaintiff's subpoena is also invalid on its face. The technology and methods utilized to identify potential Defendants are highly unreliable, leading to a significant risk of misidentification. The technology used by Plaintiffs fails to consider important factors such as persons masking false Internet Protocol ("IP") addresses, persons with hacked or open wireless networks, or computers that have been hacked by others and able to be controlled remotely. Rather, Plaintiff's technology involves use and monitoring of the Bit Torrent network to identify and collect United States IP addresses whom are allegedly downloading the content and sending those IP addresses to be added to a John Doe lawsuit for copyright infringement. Plaintiff's subpoena also impermissibly subjects Defendant to unwarranted annoyance and embarrassment. Accordingly, the present subpoena must be quashed to avoid considerable injustice.

LEGAL STANDARDS

1. AUTHORITY TO QUASH SUBPOENAS

Pursuant to Rule 45(c)(3), a Court must modify or quash a subpoena that "requires disclosure of privileged or other protected matter, if no exception or waiver applies, or subjects a person to an undue burden." A court may modify or quash a subpoena that, inter alia, requires disclosing confidential information.

Moreover, Fed. R. Civ. Pro Rule 26(c)(1), instructs the Court to limit the frequency or extent of discovery otherwise allowed by the Rules, or by local rule, if it determines that... "the burden or expense of the proposed discovery outweighs the likely benefit, considering the needs

of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of discovery in resolving the issues.”

2. STANDING

A party has standing to challenge a subpoena issued to a third party when the party has a personal or proprietary interest in the information sought by the subpoena. See *Washington v. Thurgood Marshall Acad.*, 230 F.R.D. 18, 21 (Dist. D.C., 2005).

ARGUMENT

I. PLAINTIFF'S SUBPOENA SHOULD BE QUASHED BECAUSE JOINDER OF DEFENDANTS IS IMPROPER

A. **Plaintiff Fails to Show that Claims Arise out of the Same Transaction, Occurrence, or Series of Transactions or Occurrences as Required by Federal R. Civ. Pro. 20(a) for Joinder**

Plaintiff's subpoena must be quashed because joinder is improper under Rule 20(a) of the Fed. Rules of Civil Procedure. The claims against Defendant (and those asserted against other Doe Defendants) qualify as a unique case, and are inappropriate to join because each Doe has separate network configurations, different alleged access times, separate hardware, and different ISPs, which require individual investigation and gives rise to separate and individual defenses.

Specifically, Plaintiff has failed to meet requisite elements of joinder under Fed. R. Civ. Pro. Rule 20(a). First, in Plaintiff's Complaint, Plaintiff erroneously claims that each Defendant is jointly and severally liable for the infringing activities of other Defendants without citing authority, the infringing complained of was party of a series of transactions, and was accomplished by Defendants acting in concert with one another. The claim that joinder is proper

based on Bit Torrent or other peer-to-peer (“P2P”) protocols has been reviewed and almost universally rejected by Federal Courts. *LaFace Records, L.L.C. v. Does 1-38*, 2008 U.S. Dist. LEXIS 14544, 2008 WL 544992 at 1 (rejecting Plaintiff’s argument that copyright infringement claims did not arise out of the same transaction, occurrence, or series of transactions...because each Defendant used the same ISP as well as the same P2P networks); *see also Interscope Records v. Does 1-25*, 2004 U.S. Dist. LEXIS 27782, at 2 (holding improper joinder although Defendants were alleged to have disseminated the Plaintiff’s copyrighted works through the same P2P network); *Elektra Entertainment Group, Inc. v. Does 1-9*, 2004 U.S. Dist. LEXIS 23560, 2004 WL 2095581, at 1 (finding the mere use of the same P2P protocol was insufficient to establish the Plaintiff’s copyright infringement claims were logically related for purposes of Rule 20(a)(2)); *Fonovisa, Inc. v. Does 1-9*, 2008 U.S. Dist. LEXIS 27170, 2008 WL 919701 (finding joinder improper because of the different factual contexts of the alleged infringement for each Defendant and absence a showing of any evidence showing joint action by Defendants, other than their use of the same P2P network to access copyrighted recordings); *Hard Drive Productions, Inc. v. Does 1-188*, 2011 U.S. Dist. LEXIS 94319 (holding joinder of Doe defendants improper based on alleged use of Bit Torrent Protocols); *Diabolic Video Productions v. Does 1-2,099*, U.S. Dist. LEXIS 58351, 10 (Grewal, M.J.) (N.D. Cal. May 31, 2011) (finding that the nature of the Bit Torrent protocol does not make joinder appropriate where Defendants allegedly used Bit Torrent to infringe copyrighted works. *IO Group v. Does 1-19*, 2010 U.S. Dist. LEXIS 133717, *8-9 (N.D. Cal. Dec. 7, 2010) (holding that the “only factual allegations connecting the Defendants” – the allegation that they all used the same peer-to-peer network to reproduce and distribute the Plaintiff’s copyrighted work was insufficient for joinder of multiple Defendants under Rule 20); *IO Group v. Does 1-435*, 2011 U.S. Dist. LEXIS 14123, *15-16

(N.D. Cal. Feb. 3, 2011); *Lightspeed v. Does 1-1,000*, 2011 U.S. Dist. LEXIS 35392 (N.D. Ill. Mar. 31, 2011 (Plaintiff alleged that the Defendants illegally reproduced and distributed its copyrighted works over the internet through Bit Torrent, the court severed Defendants because of improper joinder); *Boy Racer v. Does 1-71*, 2011 U.S. Dist. LEXIS 58345 (Grewal, M.J.) (N.D. Cal. May 31, 2011) (same). Although Congress may have contemplated individual suits against file sharers when considering legislative solutions to copyright infringement, they certainly did not intend for large-scale file sharing suits against individual users for allegedly acts that may be grouped together using broadly construed joinder rules.

In a recent March 2012 ruling involving Bit Torrent cases and multiple joined John Doe Defendants, a U.S. District Judge in Michigan granted Defendant's motion to quash on the grounds that an allegation of Bit Torrent use does not comport with the Rule 20(a) joinder requirements and that the Defendants were improperly joined as a matter of law. *Patrick Collins, Inc. v. John Does 1-23*, No. 2:11-cv-15231 (E.D. Michigan, Mar. 26, 2012) Dkt 8. Similar to the present facts, the case in question involved a number of John Doe Defendants, four different ISPs, and nearly three months of allegedly infringing activity. The court disagreed with Plaintiff's claims that the joinder issue should be addressed after the ISPs provide to Plaintiffs the Doe Defendants' identifying information, instead following the approach used by the Court in *Arista Records, LLC v. Does 1-11*, No. 1:07-cv-2828, 2008 U.S. Dist. LEXIS 90183, *12 (N.D. Ohio, Nov. 3, 2008). While *Arista Records* involves alleged copyright infringement utilizing P2P protocols prior to the advent of Bit Torrent, this does not change the analysis. Rule 21 of the Federal Rules of Civil Procedure provides that a court, on motion or on its own, may "at any time, on just terms, add or drop a party" or "sever any claim against a party." Fed. R. Civ. P. 21. As the court finds that the Doe Defendants have been improperly joined, allowing

Plaintiff to proceed with its lawsuit until the Doe Defendants have been identified will pervert the joinder rules. *Arista Records, LLC*, 2008 U.S. Dist. LEXIS, at *15. “Postponing a decision on joinder in lawsuits similar to this action results in lost revenue of perhaps millions of dollars and only encourages Plaintiffs and other member of the [Recording Association of America] to join (or misjoin) as many Doe Defendants as possible.” *Id.* at *17 (citing *Sony BMG Music Entm’t v. Does 1-5*, No. 07-cv-02434 (C.D. Cal., Aug. 29, 2007)).

Finally, U.S. District Judge Murray Snow for the District Court for the District of Arizona held in an almost exactly similar matter on March 19, 2012 that in order to be sued with other John Doe Defendants in Bit Torrent download cases, the individual must have either uploaded or downloaded from the other defendants in order for the first element to be met.

Plaintiff alleges that the two remaining Defendants “participat[ed] in the BitTorrent swarm with other infringers” but does not claim that John Doe 6 provided data to the former John Doe 12 or vice versa. (Doc. 26 ¶ 56)... Plaintiff has not demonstrated that John Doe 6 and the former John Doe 12 engaged in a single transaction or occurrence, or a single series of transactions or occurrences. Defendant John Doe 6 has been improperly joined, and is severed from the lawsuit. *Patrick Collins, Inc. v. John Does 1-54* (Case No. 2:12-cv-01602).

Despite Plaintiff’s claims to the contrary, Doe 4 and Defendants otherwise 1-31 herein did not participate in the same transaction or occurrence, the same series of transactions or occurrences as required by the joinder; nor, did they act in concert with one another. The fact that any of the Doe Defendants may have clicked on a command to participate in the Bit Torrent network does not mean that, each, together, was part of the downloading swarm of hundreds or thousands of individuals. Moreover, even if it were true that all Doe Defendants participate in what Plaintiff describes as a “swarm,” it cannot be stated with certainty that each Defendant was physically present at the same day and time. To the contrary, Plaintiff’s own exhibit attached to the Complaint indicates that downloading occurred at different times and dates within an eight

week range between May 17, 2012 and July 21, 2012, an almost eight week period wherein the Plaintiffs allege that Defendants were acting in concert. No statement or pleading is made as to which Doe Defendant or Defendants Doe #4 shared with or conspired with to allegedly infringe Plaintiff's work. Given that Plaintiff has failed to provide an explanation as to how each party is sharing in concert with one another, Plaintiff's Complaint is hardly sufficient to demonstrate the sufficiency of the joinder requirements of F.R.C.P. Plaintiff has not demonstrated in any way that Defendant John Doe #4 was accessing the alleged Bit Torrent tracker at the same time and transaction as the other Defendants nor have they demonstrated for how long that John Doe #4 was accessing the files if at all.

Plaintiff fails to show that the claims against each Doe Defendant arose out of the same transaction, occurrence, or series of transactions or occurrences, and therefore, Plaintiff's subpoena must be quashed.

II. PLAINTIFF'S SUBPOENA MUST BE QUASHED

A. **Defendant has Standing to Challenge the Subpoena Because Defendant Has a Personal Interest in the Subpoenaed Matter**

A party has standing to challenge a subpoena issued to a third party when the party has a personal or proprietary interest in the information sought by the subpoena. *See Washington v. Thurgood Marshall Acad.*, 230 F.R.D. 18, 21 (Dist. D.C., 2005). Here, because the subpoena issued to Comcast seeks Defendant's personally identifying information, Defendant undoubtedly has a "personal interest" in the information sought by the subpoena. Further, if Defendant's name is turned over by Comcast, Plaintiff, as part of their business model will quickly seek several settlements that amount to thousands of dollars each, with no serious intention of naming

any Defendants. If an identified Doe has a “personal or proprietary interest” sufficient to pay several thousand dollars under the threat of litigation and public exposure, certainly Defendant has a “personal or proprietary interest” sufficient to object prior to that disclosure. Accordingly, Defendant has standing to challenge the subpoena.

B. Plaintiff’s Subpoena Must be Quashed on the Basis of the Lack of Reliability relating to IP Address and MAC Address Tracking Technology

Plaintiff’s subpoena must be quashed because the technology used to identify individual Defendants for the alleged copyright infringement is unreliable and is insufficient to show a volitional act of copyright infringement. Specifically, there is not only software available that is capable of impersonating and/or falsifying an IP address, but such software is unreliable because the software does not also identify the associated computer’s MAC address at the time. An IP address can name an entire network of computers, so without the MAC address, an IP address alone is not sufficient to identify an individual accused of copyright infringement. Further, most ISPs do not store MAC address data nor do they have the ability to detect falsified or altered MAC addresses. Because the technology used by Plaintiff to identify the various John Doe Defendants is highly unreliable, Plaintiff is incapable of accurately identifying the proper individuals who actually downloaded the infringing material, and from where the material was actually downloaded. Because IP addresses are the only evidence Plaintiff has to identify Doe Defendants, Plaintiff’s subpoena is unreliable on its face and should be quashed by the Court given the evidence Plaintiff has provided thus far.

Moreover, to prove a claim for infringement, a Plaintiff must demonstrate that the Defendant copied the protected work. *Kelly v. Ariba Soft Corp.*, 336 F.3d 811, 817 (9th Cir.

2003) (“the Plaintiff must show ownership of the copyright and copying by the Defendant.”), and that the copying was a result of a volitional act. *See Religious Tech Ctr. v. Netcom On-Line Comm’n Servs., Inc.*, 907 F. Supp 1361, 1369-1370 (N.D. Cal. 1995). However, Plaintiff’s allegations are highly suspect and do not, and cannot account for numerous issues, including unsecured wireless networks, fraudulently broadcasted IP addresses, computer hacking, and more. Courts again have touched on this simple yet very logical assertion, that an IP address does not necessarily constitute a copyright infringer. Again, the *VPR* Court correctly identified this factual and legal point, observing that:

“[Plaintiff] ignores the fact that IP subscribers are not necessarily copyright infringers. 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 New York).” *VPR Internationale v. Does 1-1, 017*, No. 2:11-cv-02068, (C.D. Ill. Apr. 29, 2011), Dkt. 15, 2011 U.S. Dist. LEXIS 64656, at 3-4.

However, as noted by Judge Baker, “whether you’re guilty or not, you look like a suspect.” *Id.* at 5. (internal citations omitted).

The complaints assert that the Defendant – identified only by IP address – was the individual who downloaded the subject “work” and participated in the BitTorrent swarm. However, the 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. As one introductory guide states:

If you only connect one computer to the Internet, that computer can use the address from your ISP. Many homes today, though, use routers to share a single Internet connection between multiple computers. Wireless routers have become especially popular in recent years, avoiding the need to run network cables between rooms. If you use a router to share an Internet connection, the router gets the IP address issued directly from the ISP. Then, it creates and manages a subnet for all the computers connected to that router.²

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.

Indeed, due to the increasingly popularity of wireless routers, it is much less likely. While a decade ago, home wireless networks were nearly non-existent, 61% of US homes now have wireless access.³ Several of the ISPs at issue in this case provide a complimentary wireless router as part of Internet service. As a result, a single IP address usually supports multiple computer devices – which unlike traditional telephones can be operated simultaneously by different individuals. See *U.S. v. Latham*, 2007 WL 4563459, at *4 (D.Nev. Dec. 18, 2007). Different family members, or even visitors, could have performed the alleged downloads. Unless the wireless router has been appropriately secured (and in some cases, even if it has been secured), neighbors or passersby could access the Internet using the IP address assigned to a particular subscriber and download the plaintiff's film. In order to allow multiple computers to access the internet under the same IP address, the cable modem may be connected to a router, or may itself function as a router, which serves as a gateway through which multiple computers could access the internet at the same time under the same IP address. The router could be a wireless device in which case, computers located within 300 feet of the wireless router signal

² See "What is an IP address?" available at <http://computer.howstuffworks.com/internet/basics/question5492.htm>.

³ Lardinois, F., "Study: 61% of US Households Now Have WiFi," available at <http://techcrunch.com, 4/5/12>.

could access the internet through the router and modem under the same IP address. The wireless router signal strength could be increased beyond 600 feet if additional devices are added. The only way to prevent sharing of the wireless router is to encrypt the signal and even then an individual can bypass this security using publicly available software.

These developments cast doubt on plaintiffs' assertions that "[t]he ISP to which each Defendant subscribes can correlate the Defendant's IP address to the Defendant's true identity."

As one judge observed:

The Court is concerned about the possibility that many of the names and addresses produced in response to Plaintiff's discovery request will not in fact be those of the individuals who downloaded "[Plaintiff's movie title]." 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 "[Plaintiff's movie title]."

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

Another court noted:

the ISP subscriber to whom a certain IP address was assigned may not be the same person who used the Internet connection for illicit purposes . . . 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, placing a burden upon them that weighs against allowing the discovery as designed.

SBO Pictures, Inc. v. Does 1-3036, 2011 WL 6002620, at *3 (N.D.Cal. Nov. 30, 2011).

In sum, although the complaints state that IP addresses are assigned to "devices" and thus by discovering the individual associated with that IP address will reveal "defendants' true

identity,” this is unlikely to be the case. 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.

Moreover, Plaintiff also has the ability to pursue the Defendants in a much less intrusive manner than their current dragnet approach. Prospective Plaintiffs can file through the various ISPs notices of infringement, wherein the ISP relays via email the notice of infringement to the prospective Defendant. Plaintiffs can then attempt to settle with Defendants in a manner less expensive for all parties. If the potential Defendants fail to comply with Plaintiffs requests for settlement, Plaintiffs can then choose to sue the individuals who fail to comply. This method employed by other copyright enforcement groups creates much less of a dragnet, allows potential Defendants to remain anonymous, reduces costs to all parties, preserves precious judicial resources, and allows Plaintiffs to more efficiently identify Defendants and settle without resorting to numerous Federal lawsuits.

Based on the technological ease with which innocent individuals can be so easily falsely identified, the information in the subpoena should be viewed with skepticism. For example, when a neighbor, unbeknownst to the subscriber, illegally enables a Bit Torrent client downloading copyrighted material either remotely on the user’s computer or through an open wireless internet connection on the user’s network a subscriber can unknowingly be identified and caught up in the dragnet.

In the present circumstances, Defendant was nowhere near a computer at the time of allegedly participated in the infringing activity. Finally, there is an alternative method of copyright enforcement that Plaintiff could utilize which is less expensive than the current means

relied on by Plaintiff's broad sweeping approach. Coupled with the devastating effect of a false accusation of infringement of pornographic materials, Plaintiff's allegations fail to provide sufficient accuracy, nor an actual volitional act associated to a Defendant sufficient to support its claim, and Plaintiff's subpoena should be quashed.

C. The Subpoena Should be Quashed to Protect Defendant from Unreasonable Annoyance and Undue Burden

The Court must quash the present subpoena against John Doe #4 to prevent Defendant from suffering unwarranted annoyance and an undue burden. Fed. R. Civ. Pro.45(c)(3)(A)(iv). Presently, Plaintiff requires Defendant's confidential personally identifying information from Defendant's ISP so that Plaintiff can harass Defendant into coercing a quick and profitable settlement under the guise of publicly outing Defendant regarding an accusation of an unlawful download of pornographic material, despite questionable proof against Defendant. Plaintiff's subpoena is intended to cause an undue annoyance and hardship to Defendant, and the same would result if Defendant's personally identifying information were associated without sufficient evidentiary support with the unlawful downloading of pornographic materials. However, by quashing Plaintiff's subpoena, the Court can prevent the injustice of having Defendant unjustly harmed by questionable accusations. Given the present facts, the subpoena must be quashed.

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 at the point where it costs defendants 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 profitability 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.

WHEREFORE, Defendant respectfully requests that the Court enter an Order quashing the August 9, 2012 *subpoena duces tecum* issued to Comcast as applied to John Doe Defendant #4.

DATED: October 11, 2012

By: John Doe No. 4

John Doe No. 4

Exhibit A

AO 88B (Rev. 06/09) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

UNITED STATES DISTRICT COURT
for the District of New Jersey

MALIBU MEDIA, LLC	<i>Plaintiff</i>	Civil Action No. 1:12-cv-02069-WYD
v.		UNITED STATES DISTRICT COURT IN THE DISTRICT OF COLORADO
John Does 1 - 31,	<i>Defendants.</i>	

**SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO
PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION**

To: Comcast Corporation
Legal Demands Center
650 Centerton Road
Moorestown, NJ 08057

Production: YOU ARE COMMANDED to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and permit their inspection, copying, testing, or sampling of the material:

Please produce documents identifying the name, address, and telephone number of the defendant John Does listed in the below chart:

Doe#	IP Address	Date/Time UTC
1	107.2.239.87	5/29/2012 10:01
2	174.51.214.181	6/22/2012 6:24
3	174.51.252.65	5/25/2012 0:54
4	24.8.144.246	6/10/2012 19:17
5	24.8.235.136	5/19/2012 6:26
6	24.8.251.19	6/25/2012 3:06
7	24.8.35.167	5/26/2012 1:27
8	24.9.193.109	5/26/2012 13:24
9	24.9.254.208	5/18/2012 4:18

10	24.9.79.168	6/7/2012 7:36
11	50.134.140.26	5/30/2012 16:36
12	67.161.202.236	5/22/2012 16:33
13	67.176.100.131	6/4/2012 18:47
14	67.176.51.177	5/21/2012 0:12
15	67.176.56.183	7/21/2012 2:27
16	67.190.150.247	5/27/2012 5:08
17	67.190.20.62	5/22/2012 22:29
18	67.190.65.102	6/6/2012 21:39
19	71.196.152.51	6/10/2012 6:50
20	71.237.41.132	7/17/2012 11:01
21	75.70.180.71	6/24/2012 0:11
22	75.70.8.85	6/28/2012 12:41
23	75.70.86.37	5/20/2012 14:20
24	76.25.231.11	5/19/2012 1:13
25	76.25.255.208	6/23/2012 8:02
26	76.25.88.70	5/17/2012 23:08
27	98.245.1.74	7/11/2012 7:55
28	98.245.115.147	7/3/2012 8:36
29	98.245.41.162	5/19/2012 17:46
30	98.245.45.51	6/16/2012 5:16
31	98.245.79.196	7/5/2012 4:32

08/14/2012 07:47 FAX

003

Place: Kotzker Law Group 9609 S. University Blvd., #632134 Highlands Ranch, CO 80163	Date and Time: September 24, 2012 @ 9:30 a.m.
--	--

[] *Inspection of Premises:* YOU ARE COMMANDED to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:
--------	----------------

The provisions of Fed. R. Civ. P. 45(c), relating to your protection as a person subject to a subpoena, and Rule 45 (d) and (e), relating to your duty to respond to this subpoena and the potential consequences of not doing so, are attached.

Date: August 14, 2012

CLERK OF COURT

Signature of Clerk or Deputy Clerk

OR



Attorney's Signature

The name, address, e-mail, and telephone number of the attorney representing Plaintiff, who issues or requests this subpoena, are:
Jason Kotzker, Esq., The Kotzker Law Group, 9609 S. University Blvd., #632134, Highlands Ranch, CO 80163, Telephone: (303) 875-5386, Email: Jason@KLGIP.com

AO 88B (Rev. 06/09) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action
(page 3)

Federal Rule of Civil Procedure 45 (c), (d), and (e) (Effective 12/1/07)

(c) Protecting a Person Subject to a Subpoena.

(1) Avoiding Undue Burden or Expense;

Sanctions. A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The issuing court must enforce this duty and impose an appropriate sanction — which may include lost earnings and reasonable attorney's fees — on a party or attorney who fails to comply.

(2) Command to Produce Materials or Permit Inspection.

(A) Appearance Not Required. A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) Objections. A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing or sampling any or all of the materials or to inspecting the premises — or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

- (i) At any time, on notice to the commanded person, the serving party may move the issuing court for an order compelling production or inspection.
- (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) Quashing or Modifying a Subpoena.

- (A) When Required.** On timely motion, the issuing court must quash or modify a subpoena that:
 - (i) fails to allow a reasonable time to comply;
 - (ii) requires a person who is neither a party nor a party's officer to travel more than 100 miles from where that person resides, is employed, or regularly transacts business in person — except that, subject to Rule 45(c)(3)(B)(iii), the person may be commanded to attend a trial by traveling from any such place within the state where the trial is held;
 - (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or
 - (iv) subjects a person to undue burden.
- (B) When Permitted.** To protect a person subject to or affected by a subpoena, the issuing court may,

on motion, quash or modify the subpoena if it requires:

- (i) disclosing a trade secret or other confidential research, development, or commercial information;
- (ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party; or
- (iii) a person who is neither a party nor a party's officer to incur substantial expense to travel more than 100 miles to attend trial.

(C) Specifying Conditions as an Alternative. In the circumstances described in Rule 45(c)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

- (i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and
- (ii) ensures that the subpoenaed person will be reasonably compensated.

(d) Duties in Responding to a Subpoena.

(1) Producing Documents or Electronically Stored Information.

These procedures apply to producing documents or electronically stored information:

(A) Documents. A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) Form for Producing Electronically Stored Information Not Specified. If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) Electronically Stored Information Produced in Only One Form. The person responding need not produce the same electronically stored information in more than one form.

(D) Inaccessible Electronically Stored Information. The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) Claiming Privilege or Protection.

(A) Information Withheld. A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial preparation material must: (i) expressly make the claim; and (ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) Information Produced. If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(e) Contempt. The issuing court may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena. A nonparty's failure to obey must be excused if the subpoena purports to require the nonparty to attend or produce at a place outside the limits of Rule 45(c)(3)(A)(ii).

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 12-cv-02069-WYD-MEH

MALIBU MEDIA,

Plaintiff,

v.

JOHN DOES 1-31,

Defendants.

ORDER

Michael E. Hegarty, United States Magistrate Judge.

Before the Court is Plaintiff's Motion for Leave to Serve Third Party Subpoenas Prior to a Rule 26(f) Conference and Incorporated Memorandum of Law [filed August 8, 2012; docket #5]. Plaintiff's motion is **granted in part and denied in part**.

Plaintiff's motion alleges that the Doe Defendants, identified only by their Internet Protocol ("IP") addresses, have infringed on Plaintiff's copyrighted work by using the internet and a "BitTorrent" protocol to reproduce, distribute, display, or perform Plaintiff's protected film. Plaintiff requests permission from the Court to serve limited, immediate discovery on the Doe Defendants' Internet Service Providers ("ISPs") prior to the Rule 26(f) conference. The purpose of this discovery is to obtain additional information concerning the identities of the Doe Defendants.

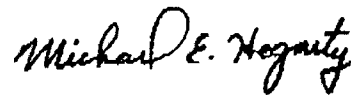
Fed. R. Civ. P. 26(d) proscribes seeking discovery before Rule 26(f) conferral. However, this prohibition is not absolute; the Court may authorize discovery upon a showing of good cause. *Pod-Ners, LLC v. Northern Feed & Bean of Lucerne Ltd. Liability Co.*, 204 F.R.D. 675, 676 (D. Colo. 2002). "Expedited discovery should be limited, however, and narrowly tailored to seek

information necessary to support expedited or preliminary relief.” *Avaya, Inc. v. Acumen Telecom Corp.*, No. 10-cv-03075-CMA-BNB , 2011 WL 9293, at *2 (D. Colo. Jan. 3, 2011) (citation omitted).

After review of the motion, the Court finds that Plaintiff establishes good cause for limited expedited discovery. Therefore, Plaintiff’s Motion for Leave to Serve Third Party Subpoenas Prior to a Rule 26(f) Conference and Incorporated Memorandum of Law [filed August 8, 2012; docket #5] is **granted in part** as follows. The Plaintiff may serve third party subpoenas pursuant to Fed. R. Civ. P. 45 on the identified ISPs with the limited purpose of ascertaining the identities of the Doe Defendants as identified by the thirty-one (31) IP addresses listed in Docket #5-4. The subpoenas shall be limited to providing Plaintiff with the true name, address, telephone number, email address, and Media Access Control address of the Defendant to whom the ISP has assigned an IP address. With each subpoena, Plaintiff shall also serve a copy of this Order. Finally, the Court emphasizes that Plaintiff may only use the information disclosed in response to the subpoenas for the purpose of protecting and enforcing its rights as set forth in its Complaint [docket #1]. The Court cautions Plaintiff that improper use of this information may result in sanctions. All other relief requested in the proposed order [docket #5-1] is **denied**.

Entered and dated at Denver, Colorado, this 9th day of August, 2012.

BY THE COURT:



Michael E. Hcgarty
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 1:12-cv-02069-WYD-MEH

MALIBU MEDIA, LLC.

Plaintiff,

v.

Does 1-31,

Defendants.

CERTIFICATE OF SERVICE

I hereby certify that on October 11, 2012, a true and correct copy of the foregoing MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANT JOHN DOE #4'S MOTION TO QUASH THE PLAINTIFF'S SUPOENA was sent via first-class mail to the following:

JASON AARON KOTZKER
KOTZKER LAW GROUP
9609 South University Boulevard
Highlands Ranch, CO 80163

DATED: October 11, 2012

By: John Doe No. 4

John Doe No. 4