1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

MALIBU MEDIA, LLC,

Plaintiff,

v.

JOHN DOE, subscriber assigned IP address 50.245.166.129,

Defendant.

/

Case No. 1:16-cv-00231-AWI-SKO

ORDER GRANTING PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY SUBPOENA PRIOR TO RULE 26(f) CONFERENCE

I. INTRODUCTION

Plaintiff Malibu Media, LLC ("Plaintiff") filed a complaint against John Doe ("Defendant") on February 17, 2016, alleging infringement claims pursuant to the United States Copyright Act of 1976. Plaintiff claims Defendant is a persistent online infringer of Plaintiff's copyrighted films. On April 7, 2016, Plaintiff filed a motion for leave to serve a third-party subpoena prior to a Rule 26(f) conference. (Doc. 6.) As Defendant has not yet been identified by name, no opposition was filed. Pursuant to Local Rule 230(g), the Court finds Plaintiff's motion suitable for decision without oral argument, and no hearing on this matter shall be set. For the reasons discussed below, Plaintiff's motion is GRANTED subject to the noted restrictions herein.

II. BACKGROUND

Plaintiff is a limited liability company that produces copyrighted adult films. Defendant is alleged to have used the BitTorrent file distribution network to download adult pornographic films subject to copyrights held by Plaintiff. Defendant has been identified in this lawsuit only by an Internet Protocol address ("IP Address") assigned to a customer on a specific date by an Internet Service Provider ("ISP") and through which the copyrighted works were allegedly downloaded.

BitTorrent technology has been described by several courts, including the district court in *Malibu Media, LLC v. Doe*, No. 15-cv-4369 (AKH), 2015 WL 4092417, *1-2 (S.D.N.Y. July 6, 2015):

> BitTorrent is a peer-to-peer file-sharing protocol that allows users to transfer large files over the internet by breaking the complete file (the "Seed") into small pieces to be downloaded in parts. Other users ("Peers") downloaded a small "torrent" file that contains an index of the pieces and directions for connecting to the Seed. When Peers connect to the Seed, they download pieces of the file at random, and begin sharing each piece once it has completed downloading. After all the pieces are downloaded, the BitTorrent software reassembles the pieces into a complete file for the Peer to view.
>
> BitTorrent is distinguishable from other file sharing protocols by its users' ability to upload and download files simultaneously. This non-sequential download structure reduces the bottleneck of traffic, which allows for faster download speeds. The Peers that are uploading and downloading the same Seed file from each other at a given point in time are collectively called a "Swarm." Members of a Swarm are able to see the IP addresses of other Peers to whom they are connected. In addition, BitTorrent "tracks" the pieces of a file as it is shared, so Peers can identify the IP addresses from which the file was downloaded.

Id. (citing *Patrick Collins, Inc. v. Doe 1*, 288 F.R.D. 233 (E.D.N.Y. 2012), *Next Phase Distribution, Inc. v. John Does 1-27*, 284 F.R.D. 165 (S.D.N.Y 2012), *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80 (E.D.N.Y. 2012)).

Plaintiff has filed a motion for leave to serve a third-party subpoena prior to a Federal Rule of Civil Procedure 26(f) discovery conference, requesting permission to initiate discovery to identify the account subscriber associated with the IP Address used to download Plaintiff's copyrighted films, notwithstanding the provision of Rule 26(d)(1) which precludes a party from seeking discovery from any source before the parties have conferred as required by Rule 26(f).

Plaintiff contends a Rule 45 subpoena to the ISP must be permitted to obtain the identity of the customer assigned the IP Address on the dates[1] in question to ascertain the identity of the person responsible for unauthorized downloading of the copyrighted works produced by Plaintiff. Plaintiff maintains there is no other way for it to obtain this information.

III. DISCUSSION

A. Legal Standard

Generally, a party may not conduct discovery before the parties have met and conferred pursuant to Federal Rule of Civil Procedure 26(f) "except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B), or when authorized by these rules, by stipulation, or by court order." Fed. R. Civ. P. 26(d)(1). The Ninth Circuit has held that when a defendant's identity is unknown at the time the complaint is filed, a court may grant the plaintiff leave to take early discovery to determine the defendant's identity "unless it is clear that discovery would not uncover the identit[y], or that the complaint would be dismissed on other grounds." *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980). District courts in the Ninth Circuit have permitted expedited discovery prior to the Rule 26(f) conference upon a showing of "good cause." *See, e.g., In re Countrywide Fin. Corp. Derivative Litig.*, 542 F. Supp. 2d 1160, 1179 (C.D. Cal. 2008) (citing *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273 (N.D. Cal. 2002)). "Good cause exists where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party." *In re Countrywide Fin. Corp. Derivative Litig.*, 542 F. Supp. 2d at 1179 (citation and quotation marks omitted).

B. Plaintiff Has Established Good Cause to Serve a Third-Party Subpoena

District courts within the Ninth Circuit have typically found good cause supporting early or expedited discovery in cases where the plaintiff alleged copyright infringement accomplished through distribution of the work over a peer-to-peer network, and where the plaintiff sought early discovery to obtain the identities and contact information of the alleged infringers from associated ISPs. *See, e.g., Berlin Media Art E.K. v. Does 1 through 146*, No. S-11-2039 KJM GGH, 2011

[1] In its complaint, Plaintiff specifically identifies 25 of its separate works that Defendant allegedly downloaded, copied, and distributed without authorization between September 30, 2014 and December 7, 2015. (Docs. 1-1 and 1-2, Exhibits A and B.)

WL 4056167, at *2 (E.D. Cal. Sept. 12, 2011) (unpublished) (granting leave to serve Rule 45 subpoena to identify doe defendant); *Malibu Media, LLC v. John Does 1-10*, No. 2:12-cv-3623-ODW (PJWx), 2012 WL 5382304 (C.D. Cal. June 27, 2012).

1. Balancing Interests in the Context of Copyright Infringement

In applying the good cause standard in cases where the unknown defendant is an anonymous internet user, courts give careful consideration to the diverging interests of both the party seeking the discovery and the unknown Doe defendant:

> With the rise of the Internet has come the ability to commit certain tortious acts, such as defamation, copyright infringement, and trademark infringement, entirely on-line. The tortfeasor can act pseudonymously or anonymously and may give fictitious or incomplete identifying information. Parties who have been injured by these acts are likely to find themselves chasing the tortfeasor from Internet Service Provider (ISP) to ISP, with little or no hope of actually discovering the identity of the tortfeasor.
>
> In such cases the traditional reluctance for permitting filings against John Doe defendants or fictitious names and the traditional enforcement of strict compliance with service requirements should be tempered by the need to provide injured parties with a[] forum in which they may seek redress for grievances. However, this need must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously. People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. This ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity.

Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999). As it pertains to copyright infringement cases involving the internet, many courts have documented growing concerns about "copyright trolls," "roughly defined as plaintiffs who are 'more focused on the business of litigation than on selling a product or service or licensing their [copyrights] to third parties to sell a product or service.'" *Malibu Media, LLC*, 2015 WL 4092417, at * 2 (quoting Matthew Sag, *Copyright Trolling, An Empirical Study*, 100 Iowa L. Rev. 1105, 1108 (2015)).

> "The paradigmatic troll plays a numbers game in which it targets hundreds or thousands of defendants, seeking quick settlements priced just low enough that it is less expensive for the defendant to pay the troll rather than defend the claim." [Matthew Sag, *Copyright Trolling, An Empirical Study*, 100 Iowa L. Rev. 1105, 1108 (2015)]. The lawsuits most frequently target anonymous John Does for alleged infringement related to the use of BitTorrent. Indeed, of "the 3,817 copyright law suits filed in 2013, over 43% were against John Does and more than three-quarters of those related to pornography." *Id.* at 1108–09. But almost none ever reaches a hearing. Rather, the "lawsuits are filed to take advantage of court ordered discovery [under Fed. R. Civ. P. 26(d)] to break the veil of anonymity that separates IP addresses from the account information of actual human beings." *Id.* at 1109; *see also Digital Sin, Inc. v. Does 1–176,* 279 F.R.D. 239, 241 (S.D.N.Y.2012). They then use this information to quickly negotiate settlements on mass scale without any intention of taking the case to trial. [footnote omitted] *See, e.g., Media Prods., Inc., DBA Devil's Film v. John Does 1–26,* No. 12–cv–3719, at 4 (S.D.N.Y. June 18, 2012) (explaining that the settlements in these BitTorrent cases are "are for notoriously low amounts relative to the possible statutory damages, but high relative to the low value of the work and minimal costs of mass litigation. Cases are almost never prosecuted beyond sending demand letters and threatening phone calls.").

Malibu Media, LLC, 2015 WL 4092417, at * 2.

The danger of copyright trolls is particularly acute in the context of pornography. In these cases, "there is a risk not only of public embarrassment for the misidentified defendant, but also that the innocent defendant may be coerced into an unjust settlement with the plaintiff to prevent the dissemination of publicity surrounding unfounded allegations." *Media Prods., Inc.*, No. 12-cv-3719, at 4; *see also Malibu Media, LLC v. Does 1-5*, No. 12-cv-2950 (JPO), 2012 WL 2001968, at *1 (S.D.N.Y. June 1, 2012) ("This Court shares the growing concern about unscrupulous tactics used by certain plaintiffs, especially in the adult film industry, to shake down the owners of specific IP addresses from which copyrighted adult films were allegedly downloaded.").

The abuses of Malibu Media in particular have been discussed by a court in the Southern District of New York:

> However, Malibu's corporate strategy relies on aggressively suing for infringement and obtaining accelerated discovery of the IP address holder's identity from the ISP. It then seeks quick, out-of-court settlements which, because they are hidden, raise serious questions about misuse of court procedure. Judges regularly complain about Malibu. For example, in May, Judge Timothy Black of the Southern District of Ohio surveyed some of Malibu's questionable conduct in

> litigations across the country. See Order to Show Cause, ECF Doc. No. 15, *Malibu Media, LLC v. Ryan Ramsey*, No. 14–cv–718 (S.D. Ohio May 26, 2015). He found that, while "Malibu Media asserts that it is necessary to invoke the Court's subpoena power to 'propound discovery in advance of a Rule 26(f) conference' . . . [,] not a single one of these 60 cases [filed in this district over the previous 12 months] has even progressed to a Rule 26(f) conference." *Id*. at 5. Indeed, most are dismissed even without the issuance of a summons. *Id*. Malibu's motive is to use the federal courts only to obtain identifying information in order to coerce fast settlements. *Id*. at 8 (citing *Malibu Media, LLC v. Does 1–54*, No. 12–cv–1407, 2012 WL 303[03]02, at *5 (D. Colo. July 25, 2012); *Malibu Media, LLC v. Does*, 923 F. Supp. 2d 1339, 1345–46 (M.D.Fla.2013)).
>
> Malibu effectuates its strategy by employing tactics clearly calculated to embarrass defendants. For example, in recent complaints filed in the Wisconsin federal courts, an attached "Exhibit C" listed additional pornographic videos downloaded to the defendants' IP addresses using BitTorrent. The titles in Exhibit C were extremely racy and lewd, and the district court sanctioned Malibu when it learned that Malibu did not even own the copyrights for the titles; rather, it had gratuitously listed them to coerce larger, faster settlements by further shaming defendants. *See Malibu Media LLC v. John Doe* subscriber assigned IP address 24.183.51.58, 2013 WL 4821911 (W.D. Wis. Sep. 10, 2013); *Malibu Media, LLC v. Doe*, No. 13–cv–536, 2013 WL 6579338, at *4 (E.D. Wis. Dec. 12, 2013).
>
> When courts have attempted to place restrictions on the subpoena to prevent Malibu from abusing the process to extort defendants, Malibu has flagrantly disregarded them. For example, after one court issued "two orders unambiguously ordering [Malibu] to file [the identified IP-registrant's name] under seal," Malibu filed it publicly anyway. Order to Show Cause, ECF Doc. No. 17, *Malibu Media, LLC v. Austen Downs*, 14–cv–707 (S.D. Ohio May 26, 2015). And in the Eastern District of New York, Magistrate Judge Gary Brown took additional precautions to protect John Doe's identity by explicitly instructing that "the subpoenaed information be sent directly to the Court, ex parte and under seal." *Patrick Collins, Inc. v. Doe 1*, 288 F.R.D. 233, 236 (E.D.N.Y. Nov. 20, 2012). Malibu instead served subpoenas that requested the identifying information be sent directly to Plaintiff's counsel. *Id*.

Malibu Media, LLC, 2015 WL 4092417, at * 4.

Despite these concerns, most district courts have permitted Plaintiff to serve ISPs with third-party subpoenas to discover the identity of the customer associated with the relevant IP Address. *See, e.g.*, *Malibu Media, LLC v. John Doe*, No. 15-cv-4381 (JFK), 2015 WL 4923114 (S.D.N.Y. Aug. 18, 2015); *Malibu Media, LLC v. John Does 1-16*, No. 12-cv-1847-AJB (DHB),

2012 WL 3809128 (S.D. Cal. Sept. 4, 2012).[2] The service of these subpoenas, however, has been subject to restrictions aimed at protecting the privacy and the interests of the individuals whose identity is discovered pursuant to the subpoenas. With this interest-balancing framework in mind, and particularly the concerns highlighted regarding these cases, the Court turns to Plaintiff's request to serve a third-party subpoena in this case and whether good cause exists to do so.

2. Good Cause Factors

In evaluating whether a plaintiff has established good cause to learn the identity of Doe defendants through early discovery, courts examine whether the plaintiff (1) identifies the Doe defendant with sufficient specificity that the court can determine that the defendant is a real person who can be sued in federal court, (2) recounts the steps previously taken to locate and identify the defendant, (3) demonstrates that the action can withstand a motion to dismiss, and (4) establishes that the discovery is likely to lead to identifying information that will permit service of process. *Columbia Ins. Co.*, 185 F.R.D. at 578-80; *Uber Technologies, Inc. v. Doe*, No. C 15-00908 LB, 2015 WL 1205167, at *2 (N.D. Cal. Mar. 16, 2015).

Here, Plaintiff has made a sufficient showing under each of the four factors to permit it to serve a third-party subpoena to identify Defendant.

a. Sufficient Specificity and Recounting Steps to Identify Defendant

Plaintiff has identified Defendant with sufficient specificity and has set forth the steps it has taken to do so. Its investigator Daniel Susac is employed by Excipio GmbH, a company that provides forensic investigation services to copyright owners. (Doc. 6-3, Susac Decl., ¶¶ 1-5.) Using forensic software, Susac was able to scan the BitTorrent file distribution network for the presence of infringing transactions involving Plaintiff's works. (Doc. 6-3, Susac Decl., ¶ 9.) A computer using the IP Address identified in Plaintiff's complaint connected to the investigator server to transmit a full copy, or portion, of the digital media files identified by the file hash values set forth in Exhibit A to the complaint.[3] (Doc. 6-3, Susac Decl., ¶ 11.) The IP Address

[2] Other district courts, however, have refused to grant Malibu Media's motion to serve a third-party subpoena. *See Malibu Media, LLC v. Doe*, No. 15-cv-4369, 2015 WL 4092417, at *4-6 (S.D.N.Y. July 6, 2015); *Malibu Media, LLC v. Doe*, No. 15-cv-1883, 2015 WL 3651566, at *2-4 (S.D.N.Y. June 5, 2015).

[3] Exhibit A contains a list of 6 hash numbers associated with particular copyrighted titles and the dates they were allegedly downloaded by Defendant. (Doc. 1-1, Exhibit A.)

identification is sufficient, at this stage, to indicate a real person used the network to download the copyrighted files. Moreover, Plaintiff sufficiently set forth the steps it has taken to locate and identify Defendant, despite that it has been unable to further identify Defendant by name. *See Hard Drive Prods., Inc. v. Does 1-118*, No. C 11-01567 LB, 2011 WL 1431612 (N.D. Cal. Apr. 14, 2011). The first two good cause factors are satisfied.

b. Sufficiency of Complaint to Withstand a Motion to Dismiss

(i) Ability to State a Claim Upon Which Relief Can Be Granted

To be entitled to early discovery, Plaintiff must establish its complaint can withstand a motion to dismiss. *Columbia Ins.*, 185 F.R.D. at 579. "Copyright is a federal law protection provided to the authors of original works of authorship." *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1106 (9th Cir. 2010) (quoting 17 U.S.C. §§ 101-103). "To establish [copyright] infringement, two elements must be proven: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original." *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 361 (1991). Plaintiff alleges it is the owner of the Copyrights-in-Suit (as identified in an exhibit to the complaint); using BitTorrent, Defendant copied and distributed constituent elements of each of the original works covered by the Copyrights-in-Suit; and Plaintiff did not permit or consent to Defendant's distribution of its works. (Doc. 1, ¶¶ 32-36.) It appears Plaintiff has stated a prima facie claim for copyright infringement that can withstand a motion to dismiss.

(ii) Personal Jurisdiction

Plaintiff bears the burden to establish jurisdictional facts, which includes personal jurisdiction over the defendant. *Columbia Ins.*, 185 F.R.D. at 579. Plaintiff has identified the IP Address associated with the allegedly infringing downloading and copying, and it is located in Fresno, California. This location is within the geographical boundaries of this judicial district. (Doc. 1, ¶ 6; Doc. 1-1, Exhibit A (identifying location of IP Address).) Further, the complaint alleges each of Defendant's acts of copyright infringement occurred in this district and that Defendant or its agents reside or may be found in this district. (Doc. 1, ¶ 8.) At this stage, it is likely that the complaint can withstand a motion to dismiss for lack of personal jurisdiction

because Defendant has an IP Address traced to a location in this district. *See 808 Holdings v. Collective of December 29, 2011*, No. 12-cv-00186, 2012 WL 1648838 (S.D. Cal. May 4, 2012).

(iii) Venue

"In copyright infringement actions, venue is proper 'in the district in which the defendant or his agent resides or may be found.'" *Brayton Purcell LLP v. Recordon & Recordon*, 606 F.3d 1124, 1128 (9th Cir. 2010) (quoting 28 U.S.C. §1400(a)). As noted above, Plaintiff has determined the alleged infringing activity occurred through an IP Address within this judicial district; thus, it is likely Plaintiff will be able to survive a motion to dismiss for improper venue under Federal Rule of Civil Procedure 12(b)(3). *See Malibu Media, LLC*, 2012 WL 3809128, at *4-5.

c. Subpoena Likely to Lead to Discovery of Identifying Information

It appears Plaintiff has obtained and investigated the available data pertaining to the alleged infringements and there is no alternative means to ascertain Defendant's identity other than by subpoenaing the ISP. (Doc. 6-1, 17:21-18:10); *Malibu Media, LLC*, 2012 WL 3809128, at *3 (IP Addresses obtained sufficiently established investigation efforts, particularly where there is no other practical measures to identify Doe defendants). The information Plaintiff seeks through service of the subpoena will likely to lead to identifying information, including Defendant's name and address, which should allow Plaintiff to effect service of process on Defendant.

In sum, Plaintiff has made a sufficient showing on all four good cause factors to permit it to pursue discovery prior to the Rule 26(f) conference.

3. Cable Privacy Act

The Cable Privacy Act, 47 U.S.C. §551, generally prohibits cable operators from disclosing personally identifiable information regarding subscribers without the prior written or electronic consent of the subscriber. 47 U.S.C. §551(c)(1). The cable operator, however, may disclose this information if the disclosure is made pursuant to a court order and the cable operator provides the subscriber with notice of the order. *Id*. § 551(c)(2)(B). The ISP Plaintiff intends to subpoena is a cable operator within the meaning of the Act.

4. Conclusion

Based on the factors discussed above, the Court finds the privacy concerns of the Defendant are balanced with the need for discovery by allowing Malibu to subpoena the ISP to discover Defendant's identity using the IP Address associated with the allegedly infringing downloads. The restrictions set forth below are intended to provide additional safeguards to Defendant's privacy interests. This Court takes very seriously the concerns noted by Judge Hellerstein of the Southern District of New York[4] and Judge Wright of the Central District of California,[5] among many others, regarding the potential for abuse in cases such as this. Although Plaintiff is permitted to serve a third-party subpoena, it is cautioned that any abuses of the judicial system or the discovery process will not be taken lightly.

IV. CONCLUSION AND ORDER

On balance of the interests involved, the Court finds Plaintiff has established good cause for the issuance of a third-party subpoena in an attempt to identify Defendant. For the reasons set forth above, IT IS HEREBY ORDERED that:

1. Plaintiff's motion to serve a third-party subpoena is GRANTED subject to the restrictions noted below;

2. Plaintiff may immediately serve a Rule 45 Subpoena ("Subpoena") on Comcast Cable to obtain information to identify Defendant John Doe, specifically his or her name and address. The ISP is **not** to release the subscriber's telephone number or email address. A copy of this Order shall be attached to the Subpoena;

3. The ISP, **Comcast Cable,** shall have 30 days from the date of service of the Subpoena upon it to serve Defendant John Doe with a copy of the Subpoena and a copy of this Order. Comcast Cable may serve Defendant using any reasonable means, including written notice sent to his or her last known address, transmitted either by first-class mail or via overnight service;

4. Defendant shall have 60 days from the date of service of the Subpoena and this Order upon him or her to file any motions with this Court contesting the Subpoena (including a

[4] *See Malibu Media, LLC*, 2015 WL 4092417.

[5] *See Malibu Media, LLC*, 2012 WL 5382304.

motion to quash or modify the Subpoena), as well as any request to litigate the Subpoena anonymously. Comcast Cable may **not** turn over the Defendant's identifying information to Plaintiff before the expiration of this 60-day period. Additionally, if the Defendant or ISP files a motion to quash the Subpoena, the ISP may not turn over any information to Plaintiff until the issues have been addressed and the Court issues an Order instructing the ISP to resume turning over the requested discovery. A Doe Defendant who moves to quash or modify the Subpoena, or to proceed anonymously, shall at the same time as her or his filing notify the ISP so that the ISP is on notice not to release any of the Defendant's contact information to Plaintiff until the Court rules on any such motions;

5. If the 60-day periods elapse without the Defendant or ISP contesting the Subpoena, the ISP shall have 10 days to produce the information responsive to the Subpoena to Plaintiff;

6. Upon service with the Subpoena, Comcast Cable shall preserve any subpoenaed information pending the resolution of any timely-filed motion to quash; and

7. Any information ultimately disclosed to Plaintiff in response to a Subpoena may be used by Plaintiff for the **sole** purpose of protecting Plaintiff's rights as set forth in the complaint.

IT IS SO ORDERED.

Dated: **May 16, 2016**

/s/ Sheila K. Oberto
UNITED STATES MAGISTRATE JUDGE