

1  
2  
3  
4  
5  
6  
7  
8 UNITED STATES DISTRICT COURT  
9 SOUTHERN DISTRICT OF CALIFORNIA  
10

11 MALIBU MEDIA, LLC,

12 Plaintiff,

13 v.

14 JOHN DOE subscriber assigned IP  
15 address 76.216.252.167,

16 Defendant.

Case No.: 3:16-cv-1914-AJB-NLS

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

**(Dkt. No. 4)**

17  
18 Before the Court is Plaintiff Malibu Media, LLC's ("Plaintiff") *Ex Parte* Motion  
19 for Leave to Serve a Third Party Subpoena Prior to a Rule 26(f) Conference. (Dkt. No.  
20 4.) No Defendant has been named or served, and so no opposition or reply briefs have  
21 been filed. For the reasons discussed below, the Court **GRANTS** Plaintiff's motion.

22 **I. Background**

23 This is one of numerous cases filed by Plaintiff alleging copyright infringement  
24 against a defendant using the BitTorrent file-sharing system. On July 28, 2016, Plaintiff  
25 filed this Complaint against "John Doe," who is allegedly a subscriber of AT&T Internet  
26 Services and assigned Internet Protocol ("IP") address 76.216.252.167 ("Defendant").  
27 (Dkt. No. 1.) Plaintiff alleges Defendant infringed its copyrights by using the BitTorrent  
28 file distribution network, one of the most common peer-to-peer file sharing systems used

1 to distribute data such as digital movie files. (Id. at ¶¶ 11, 20.) Plaintiff alleges  
2 Defendant downloaded, copied, and distributed a complete copy of Plaintiff’s works  
3 without authorization. (Id. at ¶¶ 20; 31-33; Exhs. A & B to Compl.)

4 Plaintiff seeks leave to conduct early discovery to learn the identity of the  
5 subscriber of the IP address from the Internet Service Provider (“ISP”) who leased the  
6 address. Specifically, Plaintiff seeks an order permitting it to serve a third party  
7 subpoena under Federal Rule of Civil Procedure 45 on AT&T Internet Services that  
8 would require it to supply the name and address of its subscriber to Plaintiff. (Dkt. No. 4-  
9 1 at 7.) Plaintiff does not seek the telephone number or email address of the subscriber  
10 associated with Defendant’s IP address.

## 11 **II. Legal Standard**

12 A party is generally not permitted to obtain discovery without a court order before  
13 the parties have conferred pursuant to Federal Rule of Civil Procedure 26(f). Fed. R. Civ.  
14 P. 26(d)(1). However, courts have made exceptions to allow limited discovery after a  
15 complaint is filed to permit the plaintiff to learn the identifying information necessary to  
16 serve the defendant. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 577 (N.D.  
17 Cal. 1999). A party who requests early or expedited discovery must make a showing of  
18 good cause. *See Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 275-76  
19 (N.D. Cal. 2002) (applying “the conventional standard of good cause in evaluating  
20 Plaintiff’s request for expedited discovery”). Good cause exists “where the need for  
21 expedited discovery, in consideration of the administration of justice, outweighs the  
22 prejudice to the responding party.” *Id.* at 276.

23 “The Ninth Circuit has held that when the defendants’ identities are unknown at  
24 the time the complaint is filed, courts may grant plaintiffs leave to take early discovery to  
25 determine the defendants’ identities ‘unless it is clear that discovery would not uncover  
26 the identities, or that the complaint would be dismissed on other grounds.’” 808  
27 *Holdings, LLC v. Collective of December 29, 2011 Sharing Hash*, 2012 WL 1648838, \*3  
28 (S.D. Cal. May 4, 2012) (quoting *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir.

1 1980)). “A district court’s decision to grant discovery to determine jurisdictional facts is  
2 a matter of discretion.” *Columbia Ins.*, 185 F.R.D. at 578 (citing *Wells Fargo & Co. v.*  
3 *Wells Fargo Express Co.*, 556 F.2d 406, 430 n.24 (9th Cir. 1977)).

4 To determine whether “good cause” exists to permit expedited discovery to  
5 identify John Doe defendants, district courts in this Circuit consider whether the plaintiff  
6 (1) “identif[ies] the missing party with sufficient specificity such that the Court can  
7 determine that the defendant is a real person or entity who could be sued in federal  
8 court”; (2) “identif[ies] all previous steps taken to locate the elusive defendant” to ensure  
9 that plaintiff has made a good faith effort to identify the defendant; and (3) “establish[es]  
10 to the Court’s satisfaction that plaintiff’s suit against defendant could withstand a motion  
11 to dismiss.” *Columbia Ins.*, 185 F.R.D. at 578-80. Additionally, the plaintiff should  
12 demonstrate the discovery will likely lead to identifying information that will permit  
13 service of process. *Id.* at 580. These factors are considered to ensure the expedited  
14 discovery procedure “will only be employed cases where the plaintiff has in good faith  
15 exhausted traditional avenues for identifying a civil defendant pre-service, and will  
16 prevent use of this method to harass or intimidate.” *Id.*

### 17 **III. Discussion**

#### 18 **a. Identification of Missing Party with Sufficient Specificity**

19 Plaintiff must identify Defendant with enough specificity to enable the Court to  
20 determine that Defendant is a real person or entity who would be subject to the  
21 jurisdiction of this Court. *Columbia Ins.*, 185 F.R.D. at 578. Some district courts in this  
22 Circuit have determined that “a plaintiff identifies Doe defendants with sufficient  
23 specificity by providing the unique IP addresses assigned to an individual defendant on  
24 the day of the allegedly infringing conduct, and by using ‘geolocation technology’ to  
25 trace the IP addresses to a physical point of origin.” *808 Holdings*, 2012 WL 1648838, at  
26 \*4; see *Openmind Solutions, Inc. v. Does 1-39*, 2011 U.S. Dist. LEXIS 116552, at \*6,  
27 (concluding that plaintiff satisfied the first factor by identifying the defendants’ IP  
28 addresses and by tracing the IP addresses to a point of origin within the State of

1 California); *see also Pink Lotus Entm't v. Does 1-46*, 2011 U.S. Dist. LEXIS 65614, \*6  
2 (same). Others have concluded that merely identifying the IP addresses on the day of the  
3 alleged infringement satisfies this factor. *808 Holdings*, 2012 WL 1648838, at \*4 (citing  
4 cases).

5 Here, Plaintiff provided the Court with sufficient specificity that it seeks to sue a  
6 real person subject to this Court's jurisdiction. In support of its identification of the  
7 missing party, Plaintiff provides declarations and factual contentions with evidentiary  
8 support in its complaint. Specifically, Plaintiff provides declarations from Plaintiff's  
9 investigator, Tobias Fieser who is IPP International UG's employee; from a former  
10 detective and founder of Computer Forensics, LLC, Patrick Paige; and from its counsel.

11 Mr. Fieser is an employee in the litigation support department of IPP International  
12 UG ("IPP"). IPP provides forensic investigation services to copyright owners. (Doc. No.  
13 4-4, ¶¶ 4-5.) Mr. Fieser testifies that IPP monitors the BitTorrent file distribution  
14 network to find IP addresses that are used to distribute Plaintiff's copyrighted works  
15 without authorization. (*Id.*, ¶ 6.) He attests he reviewed IPP's forensic activity logs and  
16 determined its servers connected to an electronic device using IP address 76.216.252.167  
17 and that the IPP software determined that IP address was distributing digital content that  
18 was "substantially similar to Malibu Media's copyrighted movie" titled "Triple Blonde  
19 Fantasy." (*Id.*, ¶¶ 9-11.) These monitoring efforts indicated that the IP address at issue  
20 transmitted copies or portions of copies of Plaintiff's copyrighted work at a specific date  
21 and time. (*Id.*) He further attests he verified a "TCP/IP" connection was made between  
22 his company's investigative servers and the electronic device using Defendant's IP  
23 address, such that it was impossible that another party was "spoofing" the Defendant's IP  
24 address.<sup>1</sup> (*Id.*, ¶ 13.)

---

25  
26  
27 <sup>1</sup> "Spoofing" in computer terminology refers to "tricking or deceiving computer systems  
28 or other computer users. This is typically done by hiding one's identity or faking the  
identity of another user on the Internet.... [IP spoofing] involves masking the IP address

1 Mr. Paige attests that in his experience, during the initial phase of Internet based  
2 investigations the offender is only known by an IP address. (Doc. No. 4-3, ¶ 13.) He  
3 contends that “[t]he only entity able to correlate an IP address to a specific individual at a  
4 given date and time is the Internet Service Provider (‘ISP’).” (Id., ¶ 14.) He further  
5 declares that he tested IPP’s infringement detection system for its accuracy, determined  
6 IPP’s system accurately recorded the names and version numbers of the test computers he  
7 set up, and he concluded that IPP’s system accurately works. (Id., ¶¶ 29, 39, 41-42.)

8 The factual contentions in Plaintiff’s Complaint trace the allegedly offending IP  
9 address to this District. Plaintiff states that it “used proven IP address geolocation  
10 technology which has consistently worked in similar cases to ensure that the Defendant’s  
11 acts of copyright infringement occurred using an Internet Protocol address (“IP address”)  
12 traced to a physical address located within this District.” (Doc. No. 1, ¶ 5.) Additionally,  
13 Plaintiff’s counsel submitted a declaration that Plaintiff used Maxmind Premium’s IP  
14 geolocation database to trace the IP address to a location inside this District. (Doc. No.  
15 4-6, ¶¶ 7-9.) He attests that Plaintiff traced Defendant’s IP address approximately three  
16 weeks before this action, and a second time immediately before filing the action to avoid  
17 any issues with dynamic IP addresses, and that the IP address traced to this District each  
18 time. (Id., ¶¶ 12-13.)

19 Based on this evidence and information, the Court finds Plaintiff satisfied the  
20 “sufficient specificity” threshold. Plaintiff provides the Court with information about the  
21 allegedly infringing activity at a particular IP address, including the dates and times of  
22 particular infringing activity. (Doc. No. 1-1 (Exh. A. to the Complaint).) Plaintiff also  
23 states in its Complaint that it narrowed the activity to a specific IP address, and that it  
24

25  
26 of a certain computer system. By hiding or faking a computer’s IP address, it is difficult  
27 for other systems to determine where the computer is transmitting data from.”  
28 Christensson, P. (Nov. 13, 2007). *Spoofing Definition*, retrieved Oct. 21 2016, from  
<http://techterms.com>.

1 used geolocation technology to trace the identified IP address to within this District.  
2 Accordingly, the Court concludes Plaintiff provided a sufficient showing that it seeks to  
3 sue a real person subject to the Court’s jurisdiction. Likewise, if Plaintiff obtains the  
4 identifying information from the ISP for the subscriber assigned the IP address at issue,  
5 the information sought in the subpoena would likely enable Plaintiff to serve the  
6 Defendant.

7 **b. Previous Attempts to Locate Defendants**

8 Second, Plaintiff must describe all previous steps taken to locate the Defendant to  
9 ensure that Plaintiff made a good faith effort to identify the Defendant. Here, Plaintiff  
10 states that it diligently attempted to locate Defendant by searching for Defendant’s IP  
11 address using online search engines. Plaintiff also states it engaged in diligent research to  
12 attempt to identify Defendant using other means, and also extensively discussed this issue  
13 with its computer forensics investigator. Plaintiff states that despite its diligent efforts, it  
14 is unable to identify any means of obtaining the identity of the Defendant other than  
15 through subpoenaing the information from the ISP. (Dkt. No. 4-1 at 15; *see also* Dkt.  
16 No. 4-3 at ¶ 14 (“the only entity able to correlate an IP address to a specific individual at  
17 a given date and time is the Internet Service Provider (‘ISP’).”). In light of this  
18 information, the Court finds Plaintiff made a good faith effort to identify and locate the  
19 Defendant.

20 **c. Whether Plaintiff Can Withstand a Motion to Dismiss**

21 To survive a motion to dismiss, Plaintiff must make a *prima facie* case of copyright  
22 infringement. A plaintiff must show: (1) ownership of a valid copyright; and (2) that  
23 Defendant violated the copyright owner’s exclusive rights under the Copyright Act.  
24 *Range Road Music, Inc. v. East Coast Foods, Inc.*, 668 F.3d 1148, 1153 (9th Cir. 2012).  
25 Here, Plaintiff alleges it is the owner of the copyrights-in-suit. (Dkt. No. 1 at ¶¶ 25, 31.)  
26 Plaintiff also submits declarations from Colette Pelissier, owner of Malibu Media, and  
27 Erin Sinclair, the Chief Operating Officer. Ms. Pelissier attests each of the works were  
28 downloaded and compared side by side to a control copy of Malibu Media’s works.

1 (Dkt. No. 4-2, ¶ 18.) Ms. Sinclair attests that the works in the “Unauthorized Packs”  
2 transmitted by the IP address at issue are identical, strikingly similar or substantially  
3 similar to Malibu Media’s original copyrighted works. (Dkt. No. 4-5 at ¶12.) Plaintiff  
4 also alleges that Defendant used BitTorrent to copy and distribute the elements of the  
5 original works covered by the copyrights-in-suit without authorization. (Dkt. No. 1 at ¶¶  
6 31-33.)

7         Additionally, Plaintiff alleges sufficient facts to show it can withstand a motion to  
8 dismiss for lack of personal jurisdiction and withstand a motion for improper venue  
9 because Defendant’s IP address was traced to a location in this District. (Dkt. No. 1 at ¶¶  
10 5-7.) Accordingly, the Court concludes Plaintiff has alleged a *prima facie* showing of  
11 copyright infringement that would likely withstand a motion to dismiss.

#### 12                     **d. Additional Considerations**

13         Notwithstanding the above conclusions, the Court notes the growing concerns  
14 about “copyright trolls,” which are “roughly defined as plaintiffs who are ‘more focused  
15 on the business of litigation than on selling a product or service or licensing their  
16 [copyrights] to third parties to sell a product or service.’” *Malibu Media, LLC v. Doe*,  
17 2015 U.S. Dist. LEXIS 87751, \* 2 (S.D.N.Y. July 6, 2015) (*quoting* Matthew Sag,  
18 Copyright Trolling, An Empirical Study, 100 Iowa L. Rev. 1105, 1108 (2015)). As one  
19 district court recently noted, the “danger of copyright trolls is particularly acute in the  
20 context of pornography.” *Malibu Media, LLC v. Doe*, 2016 U.S. Dist. LEXIS 35534  
21 (E.D. Cal. Mar. 18, 2016). “In these cases, ‘there is a risk not only of public  
22 embarrassment for the misidentified defendant, but also that the innocent defendant may  
23 be coerced into an unjust settlement with the plaintiff to prevent the dissemination of  
24 publicity surrounding unfounded allegations.’” *Id.* (*quoting Media Prods., Inc. v. Doe*,  
25 2012 U.S. Dist. LEXIS 84111, at \*4 (S.D.N.Y. June 18, 2012).<sup>2</sup> Indeed, other courts have

---

26  
27  
28 <sup>2</sup> This is particularly so because “[t]he fact that a copyrighted work was illegally  
downloaded from a certain IP address does not necessarily mean that the owner of that IP

1 examined and recounted instances of Malibu Media’s abuse of court process and  
2 questionable conduct in its litigations across the country. *See Malibu Media, LLC v. Doe*,  
3 2016 U.S. Dist. LEXIS 35534, \*9-12 (E.D. Cal. Mar. 18, 2016) (providing excerpts from  
4 a Southern District of New York case, *Malibu Media, LLC v. Doe*, 2015 U.S. Dist.  
5 LEXIS 87751 (S.D.N.Y. July 6, 2015), which discussed Malibu Media’s abuses of  
6 process).

7 This Court likewise “shares the growing concern about unscrupulous tactics used  
8 by certain plaintiffs, especially in the adult film industry, to shake down the owners of IP  
9 addresses” to exact quick and quiet settlements from possibly innocent defendants who  
10 pay out only to avoid potential embarrassment. *Malibu Media, LLC v. Does 1-5*, 2012  
11 U.S. Dist. LEXIS 77469, \*1 (S.D.N.Y. June 1, 2012). Here, Plaintiff has nonetheless  
12 sought to alleviate these concerns by submitting a declaration from Collette Pelissier.  
13 Ms. Pelissier states Malibu Media solely seeks to protect its frequently infringed  
14 copyrights and does not seek to use the court system to profit from infringement. (Dkt.  
15 No. 4-2 at ¶ 25.) She further attests she instructs her legal team to be open to exculpatory  
16 evidence and to be cautiously prudent when pursuing these claims. (Dkt. No. 4-2 at ¶  
17 20.) Plaintiff also states that it does not solicit settlements before serving a defendant and  
18 will only settle before service where the defendant initiates the request. (Dkt. No. 4-1 at  
19 9.) Plaintiff also states it will not object to the Court imposing conditions it deems  
20 necessary to protect against any perceived concerns, such as by allowing the defendant to  
21

---

22  
23 address was the infringer. Indeed, the true infringer could just as easily be a third party  
24 who had access to the internet connection, such as a son or daughter, houseguest,  
25 neighbor, or customer of a business offering internet connection.” *Malibu Media, LLC v.*  
26 *Doe*, 2015 U.S. Dist. LEXIS 87751, \*14 (S.D.N.Y. July 6, 2015) (*quoting Patrick*  
27 *Collins, Inc. v. Does 1-6*, 2012 U.S. Dist. LEXIS 77486 \*1 (S.D.N.Y. June 1, 2012)  
28 (internal citations omitted). Nonetheless, it is not clear to this Court how Plaintiff could  
discover this information without first identifying the subscriber to the IP address and  
making appropriate inquiries. *Dead Season LLC v. Doe*, 2013 U.S. Dist. LEXIS 101993,  
\*16 (D. Ariz. July 19, 2013) (concluding the same).



1 litigate through discovery anonymously. (Id.) Given Ms. Pelissier and Plaintiff's  
2 counsel's representations that it will not engage in unscrupulous settlement tactics, the  
3 Court does not find conditions to prevent such tactics are necessary at this time.  
4 However, to protect from embarrassment the possibly innocent defendant, the Court will  
5 set forth conditions below intended to provide additional safeguards to the process. *See*  
6 *e.g., Malibu Media v. Doe*, 2014 U.S. Dist. Lexis 79595, \*5 (M.D. Fla. Apr. 10, 2014)  
7 (imposing similar conditions and citing cases that do the same); *see also Malibu Media,*  
8 *LLC v. Doe*, 2016 U.S. Dist. LEXIS 35534, \*17 (E.D. Cal. Mar. 18, 2016).

#### 9 **IV. Conclusion**

10 For good cause shown, the Court **GRANTS** Plaintiff's *ex parte* motion for leave to  
11 serve a subpoena prior to a Rule 26(f) conference. It is **ORDERED** that:

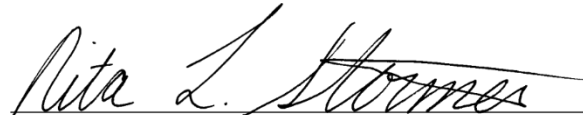
- 12 1. Plaintiff may serve the ISP with a Rule 45 subpoena commanding the ISP to  
13 provide Plaintiff with **only** the true name and address of the Defendant to  
14 whom the ISP assigned an IP address as set forth on Exhibit A to the  
15 Complaint. The ISP is **not** to release the Defendant's telephone number or  
16 email address. Plaintiff shall attach to any such subpoena a copy of this  
17 Order.
- 18 2. Within fourteen (14) calendar days after service of the subpoena, the ISP  
19 shall notify the subscriber that his or her identity has been subpoenaed by  
20 Plaintiff. The ISP must also provide a copy of this Order along with the  
21 required notice to the subscriber whose identity is sought pursuant to this  
22 Order.
- 23 3. The subscriber whose identity has been subpoenaed shall have thirty (30)  
24 calendar days from the date of such notice to challenge the disclosure of his  
25 or her name and contact information by filing an appropriate pleading with  
26 this Court contesting the subpoena. A subscriber who moves to quash or  
27 modify the subpoena may proceed anonymously as "John Doe," and shall  
28

1 remain anonymous until the Court orders that the identifying information  
2 can be released.

- 3 4. If the ISP wishes to move to quash the subpoena, it shall do so before the  
4 return date of the subpoena. The return date of the subpoena must allow for  
5 at least forty-five (45) days from service to production. If a motion to quash  
6 or other challenge is brought, the ISP shall preserve the information sought  
7 by Plaintiff in the subpoena pending resolution of such motion or challenge.  
8 5. Plaintiff may only use the information disclosed in response to a Rule 45  
9 subpoena served on the ISP for the purpose of protecting and enforcing  
10 Plaintiff's rights as set forth in its Complaint. If the Defendant wishes to  
11 proceed anonymously, Plaintiff may not release any identifying information  
12 without a court order allowing the release of the information.

13 **IT IS SO ORDERED.**

14 Dated: October 26, 2016



Hon. Nita L. Stormes  
United States Magistrate Judge