

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 107.222.125.20,

16 Defendant.

Case No.: 16-CV-0427-WQH (WVG)

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

17  
18 The Ex Parte Motion for Leave to Serve a Third Party Subpoena Prior to a Rule 26(f)  
19 Conference is GRANTED. (Doc. No. 4.)

20 1. BACKGROUND

21 Plaintiff Malibu Media, LLC (“Plaintiff”) filed this lawsuit on February 18, 2016,  
22 against John Doe Defendant (“Defendant”). Plaintiff alleges that it “only knows Defendant  
23 by his, her or its IP address.” (Doc. No. 1, ¶10.) Plaintiff seeks recovery against Defendant  
24 for “persistent online infringe[ment] of Plaintiff’s copyrights.” (Doc. No. 1, ¶2.) Plaintiff  
25 represents that it is the registered owner of various movies, which Defendant illegally  
26 “downloaded, copied, and distributed ... without authorization.” (Doc. No. 1, ¶21.)

27 Plaintiff alleges that Defendant infringed its copyrighted works using the BitTorrent  
28 File Distribution Network. In order for users of the BitTorrent File Distribution Network

1 to share files, “BitTorrent protocol breaks a file into many small pieces. Users then  
2 exchange these small pieces among each other instead of attempting to distribute a much  
3 larger digital file.” (Doc. No. 1, ¶14.) Each digital media file “has a unique cryptographic  
4 hash value ... which acts as a digital fingerprint identifying the digital media file” such as  
5 a movie. (Doc. No. 1, ¶18.) Each piece of the broken down file is also assigned a unique  
6 cryptographic hash value. (Doc. No. 1, ¶16.)

7 Plaintiff traced Defendant’s IP address from the BitTorrent File Distribution  
8 Network using an investigator, who established a direct TCP/IP connection with  
9 Defendant’s IP address. (Doc. No. 1, ¶19.) The investigator then downloaded one or more  
10 pieces of each of the alleged infringing digital media files. (Doc. No. 1, ¶20.) Plaintiff’s  
11 investigator also verified that the unique cryptographic hash values corresponded to works  
12 copyrighted by Plaintiff and that the downloaded files were identical (or strikingly similar  
13 or substantially similar) to copies of Plaintiff’s works. (Doc. No. 1, ¶22-25.) Plaintiff then  
14 connected Defendant’s IP address to a location in this district using “proven IP address  
15 geolocation technology.” (Doc. No. 1, ¶6.)

16 Although there has been no Rule 26(f) conference in this matter, nor has discovery  
17 begun, Plaintiff seeks expedited discovery. Plaintiff requests that the Court allow Plaintiff  
18 to serve a subpoena upon Defendant’s Internet Service Provider<sup>1</sup> (“ISP”) to learn  
19 Defendant’s true name and address.<sup>2</sup> (See Doc. No. 4.) Plaintiff argues that there is good  
20 cause to allow the subpoena at this early juncture because it has “no [alternative] way to  
21 ascertain Defendant’s identity” and there is risk that the ISP will destroy the records that  
22 reveal the information. (Doc. No. 4-1 at 16.)

---

23  
24  
25  
26 <sup>1</sup> Plaintiff seeks to serve AT&T Internet Services as Defendant’s ISP. (Doc. No. 4-5 at 1.)

27 <sup>2</sup> Under the Cable Privacy Act, a cable operator may disclose personally identifiable  
28 information without prior consent of the subscriber if the disclosure is made pursuant to a  
court order and the cable operator provides the subscriber with notice of the order. 47  
U.S.C. § 551(c)(2)(B).

1           2. ANALYSIS & RULING

2           a. Expedited Discovery Requires Good Cause

3           Under Federal Rule of Civil Procedure 26(d)(1), a party must seek a court order to  
4 conduct expedited discovery prior to a Rule 26(f) conference between the parties. Fed. R.  
5 Civ. Proc. § 26(d)(1). In the Ninth Circuit, a party must demonstrate “good cause” in order  
6 to obtain such an order. *Semitol, Inc. v. Tokyo Electron America, Inc.*, 208 F.R.D. 273, 276  
7 (N.D. Cal. 2002) (adopting the “good cause” standard in evaluating a request for expedited  
8 discovery). Good cause exists “where the need for expedited discovery, in consideration of  
9 the administration of justice, outweighs the prejudice to the responding party.” *Id.*

10           b. Courts Apply a Three Factor Test to Determine Whether Good Cause Exists

11           A three-factor test is applied to determine whether a party has demonstrated good  
12 cause. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999). The  
13 party must first “identify the missing party with sufficient specificity such that the Court  
14 can determine that the defendant is a real person or entity who could be sued in federal  
15 court.” *Id.* Second, the party must describe “all previous steps taken to locate the elusive  
16 defendant” to ensure that he or she has made a good faith effort to identify the defendant.  
17 *Id.* Lastly, the party must establish that the lawsuit could withstand a motion to dismiss. *Id.*  
18 Where, as here, a plaintiff seeks expedited discovery to identify an infringing user of an IP  
19 address, Courts frequently find good cause. *See UMG Recordings, Inc. v. Doe*, C08-1193-  
20 SBA, 2008 WL 4104207, \*3 (N.D. Cal. Sept. 3, 2008) (granting leave to take expedited  
21 discovery for documents that would reveal the identity and contact information for each  
22 Doe defendant); *see also Malibu Media, LLC, v. John Does 1-10*, 12-cv-3623ODW, 2012  
23 WL 5832304 (C.D. Cal. Jun. 27, 2012) (same); *Capitol Records, Inc. et al. v. John Doe*,  
24 07cv1570JM(POR), 2007 WL 2429830 (S.D. Cal. Aug. 24, 2007) (same).

25           i. Identification of Missing Party with Sufficient Specificity

26           The first prong of the three factor “good cause” test requires Plaintiff to identify  
27 Defendant with sufficient specificity such that the Court can determine he or she is a real  
28 person subject to the Court’s jurisdiction. *Columbia Ins. Co.*, 185 F.R.D. at 578-80. Here,

1 Plaintiff provides several supporting declarations, including from a BitTorrent investigator,  
2 Daniel Susac, and another from Patrick Paige, a former detective in the Palm Beach County  
3 Sheriff's Department and founder of Computer Forensics, LLC. (Doc. No. 4-3, 4-4.)  
4 Plaintiff's Complaint also provides key information linking the IP address in question to  
5 this district.<sup>3</sup>

6 Mr. Susac states that he serves in the litigation support department of Excipio  
7 GmbH, a forensic investigation service company. (Doc. No. 4-3, ¶ 4-5.) Excipio GmbH  
8 "routinely monitors" the BitTorrent file distribution network to find IP addresses being  
9 used to distribute Plaintiff's copyrighted works without authorization. (Doc. No. 4-3, ¶ 6-  
10 7.) Mr. Susac used forensic software called Network Activity Recording and Supervision  
11 ("NARS") to scan the BitTorrent network for infringing activity involving Plaintiff's  
12 copyrighted works. (Doc. No. 4-3, ¶8-15.) These monitoring efforts and use of the NARS  
13 software revealed that the IP address at issue in this lawsuit transmitted copies or portions  
14 of copies of Plaintiff's copyrighted works at specific dates and times. (*Id.*; Doc. No. 1-2.)

15 Mr. Paige's testimony proffers that an IP address is sufficient means to identify the  
16 user behind it. (Doc. No. 4-4, ¶10,11.) He contends that "[t]he only entity able to correlate  
17 an IP address to a specific individual at a given date and time is the Internet Service  
18 Provider." (*Id.*) He also states that only in one instance, of approximately 200 during his  
19 tenure in the Computer Crimes Unit, was he unable to link the IP address to the alleged  
20 person behind the unlawful activity. (Doc. No. 4-4, ¶12-13.)

21 Plaintiff's Complaint traces the offending IP address to this district. Plaintiff states  
22 that it "used proven IP address geolocation technology, which has consistently worked in  
23 similar cases, to ensure that the Defendant's acts of copyright infringement occurred using  
24 an Internet Protocol address ("IP address") traced to a physical address located within this  
25 District." (Doc. No. 1, ¶6.)

---

26  
27 <sup>3</sup> By signing the Complaint, counsel for Plaintiff has represented that the factual contentions therein  
28 (including Plaintiff's use of geolocation technology to link the IP address at issue to this district) "have  
evidentiary support." Fed. R. Civ. Proc. 11(b)(2).

1           Based on this evidence and information, the Court finds that Plaintiff has satisfied  
2 the “sufficient specificity” threshold. Plaintiff provides the Court with information about  
3 infringing activity at a particular IP address including the dates and times of particular  
4 infringing activity. (Doc. No. 1-2.) Plaintiff has narrowed the activity to a specific IP  
5 address, which for some courts, the IP address alone has been sufficient to satisfy the  
6 “sufficiently specific” prong. *See MCGIP, LLC v. Does 1-149*, C11-2331LB, 2011 WL  
7 3607666 at \*2 (N.D. Cal. Aug. 15, 2011). Moreover, Plaintiff also informs the Court that  
8 it used geolocation technology to trace the identified IP address to this district. *See Pink*  
9 *Lotus Entertainment, LLC v. Does 1-46*, No.C11-2263HRL, 2011 WL 2470986 (N.D. Cal.  
10 Jun. 21, 2011) (finding that allegation of geolocation technology use in complaint meets  
11 ‘sufficiently specific’ standard).<sup>4</sup> In aggregate, Plaintiff has provided the Court with  
12 sufficient reassurance that it seeks to sue a real person subject to the Court’s jurisdiction.

13                           ii. Previous Attempts to Locate Defendant

14           In order to satisfy the second prong of the “good cause” standard, Plaintiff must  
15 describe all prior attempts to identify the Defendant and demonstrate a good faith effort to  
16 locate and effect service of the Complaint. Here, as recorded in the Declaration of Mr.  
17 Susac, Plaintiff hired a computer investigation company to “routinely monitor” the  
18 BitTorrent network and identify the IP addresses of BitTorrent users, like Defendant, who  
19 allegedly infringed upon Plaintiff’s copyrighted material. (Doc. No. 4-3, ¶¶ 6-16.) However,  
20 as explained by Mr. Paige, based on his experience, “[t]he only entity able to correlate an  
21 IP address to a specific individual at a given date and time is the Internet Service Provider.”  
22 (Doc. No. 4-4, ¶10.) Plaintiff also notes its unsuccessful efforts to utilize various web  
23 search tools such as Google to try and find Defendant using the IP address. (Doc. No. 4-1.  
24 at 21:17-27.) The Court therefore finds that Plaintiff has made a good faith effort to identify  
25 and locate Defendant.

26  
27  
28  

---

<sup>4</sup> See Footnote 3, concerning the Federal Rules of Civil Procedure.

1                   iii. Whether Plaintiff Can Withstand a Motion to Dismiss

2           Plaintiff alleges direct copyright infringement. In order to survive a motion to  
3 dismiss, Plaintiff must demonstrate (1) ownership of a valid copyright; and (2) that  
4 Defendant violated the copyright owner’s exclusive rights under the Copyright Act. *See*  
5 *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (citing 17 U.S.C. § 501(a)  
6 (2003); *Ets-Hokin v. Skyy Spirits, Inc.*, 225 F.3d 1068, 1073 (9th Cir. 2000)). Here, Plaintiff  
7 purports to hold rights to the copyrighted works at issue. (Doc. No. 1, ¶4, 22, 32, Doc. No.  
8 1-3.) Plaintiff alleges that between October 2014 and December 2015, Defendant used the  
9 BitTorrent File Distribution Network to “download[], cop[y], and distribut[e] a complete  
10 copy of Plaintiff’s works without authorization.” (Doc. No. 1, ¶21.) As such, the Court  
11 finds that Plaintiff has alleged the prima facie elements of direct copyright infringement  
12 that would likely withstand a motion to dismiss. *See Columbia Ins. Co.*, 185 F.R.D. at 579-  
13 80.

14           3. CONCLUSION & ORDER

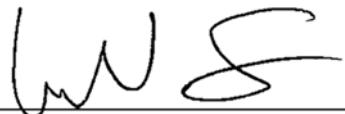
15 Having found good cause, the Court GRANTS Plaintiff’s motion for expedited discovery.  
16 For the foregoing reasons, it is hereby ORDERED that:

- 17           a. Plaintiff may serve a subpoena pursuant to Fed. R. Civ. P. 45, on AT&T  
18 Internet Services that seeks only the true name and address of Defendant.  
19 Plaintiff may not subpoena additional information;
- 20           b. Plaintiff may only use the disclosed information for the sole purpose of  
21 protecting its rights in pursuing this litigation;
- 22           c. Within fourteen (14) calendar days after service of the subpoena, AT&T  
23 Internet Services shall notify the subscriber that its identity has been  
24 subpoenaed by Plaintiff. The subscriber whose identity has been subpoenaed  
25 shall have thirty (30) calendar days from the date of such notice to challenge  
26 the disclosure by filing an appropriate pleading with this Court contesting the  
27 subpoena;
- 28

- 1 d. If AT&T Internet Services wishes to move to quash the subpoena, it shall do  
2 so before the return date of the subpoena. The return date of the subpoena  
3 must allow for at least forty five (45) days from service to production. If a  
4 motion to quash or other customer challenge is brought, AT&T Internet  
5 Services shall preserve the information sought by Plaintiff in the subpoena  
6 pending resolution of such motion or challenge; and  
7 e. Plaintiff shall serve a copy of this Order with any subpoena obtained and  
8 served pursuant to this Order to AT&T Internet Services. AT&T Internet  
9 Services, in turn, must provide a copy of this Order along with the required  
10 notice to the subscriber whose identity is sought pursuant to this Order.

11 IT IS SO ORDERED.

12 Dated: March 23, 2016

13   
14 \_\_\_\_\_  
15 Hon. William V. Gallo  
16 United States Magistrate Judge  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28