

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  
SOUTHERN DISTRICT OF CALIFORNIA

STRIKE 3 HOLDINGS, LLC,  
Plaintiff,  
v.  
JOHN DOE, subscriber assigned IP  
address 99.26.121.221,  
Defendant.

Case No.: 20CV2118 GPC (BGS)

**ORDER GRANTING EX PARTE  
APPLICATION FOR LEAVE TO  
SERVE THIRD PARTY SUBPOENA  
PRIOR TO RULE 26(F)  
CONFERENCE**

**[ECF 4]**

Plaintiff Strike 3 Holdings, LLC’s *Ex Parte* Applications for Leave to Serve a Third Party Subpoena Prior to a Rule 26(f) Conference is **GRANTED**.

**I. BACKGROUND**

On October 28, 2020, Strike 3 Holdings, LLC (“Plaintiff”) filed its Complaint against Defendant John Doe subscriber assigned Internet Protocol (“IP”) address 99.26.121.221 (“Doe Defendant”) for copyright infringement. (Compl. [ECF No. 1].) On November 12, 2020, Plaintiff filed an *Ex Parte* Application seeking leave to serve a third-party subpoena to ascertain the identity of the Doe Defendant. (*Ex Parte* Appl. [ECF No. 4].)

In its Complaint, Plaintiff asserts that Defendant is liable for direct copyright infringement. (Compl. ¶¶ 48-53.) Plaintiff alleges it owns the copyrights for movies it

1 distributes through adult websites and DVD sales. (*Id.* ¶¶ 3, 14.) Plaintiff alleges Doe  
2 Defendant used BitTorrent, a peer-to-peer file sharing system, to copy and distribute its  
3 movies without consent. (*Id.* ¶¶ 18-42.) As discussed further below, to identify the IP  
4 address that was illegally distributing its works, Plaintiff utilized its proprietary forensic  
5 software, VXN Scan (“VXN”). (*Id.* ¶¶ 28-40; *Ex Parte* Appl. at 1.)

6 As it can only identify the Doe Defendant by the IP address used, Plaintiff requests  
7 permission to serve a Federal Rule of Civil Procedure 45 subpoena on the Internet Service  
8 Provider (“ISP”), AT&T U-Verse, that issued the IP address to Doe Defendant. (*Ex Parte*  
9 Appl. at 1-2.) The proposed subpoena only demands the name and address of Doe  
10 Defendant, and Plaintiff indicates it will only use this information to prosecute claims in  
11 the Complaint. (*Id.* at 2.)

12 Plaintiff claims good cause exists to grant the *Ex Parte* Application because:  
13 (1) Plaintiff has identified Doe Defendant with sufficient specificity through geolocation  
14 technology and forensic investigation; (2) Plaintiff has identified all previous steps taken  
15 to locate Doe Defendant; (3) Plaintiff’s Complaint could withstand a motion to dismiss;  
16 and (4) Plaintiff has established that there is a reasonable likelihood that Plaintiff can  
17 identify the Doe Defendant and effectuate service. (*Id.* at 5-12.)

## 18 **II. STANDARD OF REVIEW**

19 Absent a court order, discovery is generally not allowed prior to the parties’ Federal  
20 Rule of Civil Procedure 26(f) conference. *See* Fed. R. Civ. P. 26(d)(1). Early discovery  
21 to identify a defendant may be warranted given “a plaintiff cannot have a discovery  
22 planning conference with an anonymous defendant.” *UMG Recordings, Inc. v. Doe*, No.  
23 C-08-03999-RMW, 2008 WL 4104207, at \*2 (N.D. Cal. Sept. 4, 2008). To determine if  
24 early discovery is warranted in a particular case, the court applies a “good cause” test by  
25 weighing the need for discovery to further justice against the prejudice it may cause the  
26 opposing party. *Semitoool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 276 (N.D. Cal.  
27 2002); *see also Strike 3 Holdings, LLC v. Doe*, No. 17CV2317 JAH (BLM), 2017 WL  
28 6389848, at \*1 (S.D. Cal. Dec. 14, 2017) (citing *Semitoool*, 208 F.R.D. at 274).

1 The Ninth Circuit has held that when a defendant’s identity is unknown at the time  
2 a complaint is filed, courts may grant a plaintiff leave to take early discovery to determine  
3 the defendant’s identity “unless it is clear that discovery would not uncover the identit[y],  
4 or that the complaint would be dismissed on other grounds.” *Gillespie v. Civiletti*, 629  
5 F.2d 637, 642 (9th Cir. 1980). In determining whether to grant leave for early discovery  
6 to ascertain a defendant’s identity, district courts consider: (1) whether the plaintiff can  
7 “identify the missing party with sufficient specificity such that the defendant is a real  
8 person or entity who could be sued in federal court”; (2) whether the plaintiff has described  
9 “all previous steps taken to locate the elusive defendant”; (3) whether the “suit against  
10 defendant could withstand a motion to dismiss”; and (4) whether the requested “discovery  
11 process would lead to identifying information about [the] defendant that would make  
12 service of process possible.” *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578-  
13 80 (N.D. Cal. 1999).

### 14 **III. DISCUSSION**

#### 15 **A. Identification of the Doe Defendant with Sufficient Specificity**

16 Plaintiff has identified the Doe Defendant with sufficient specificity to enable the  
17 Court to determine if Doe Defendant is a real person, subject to the Court’s jurisdiction.  
18 *Columbia Ins.*, 185 F.R.D. at 578; *see also Distinct Media Limited v. Doe Defendants 1-*  
19 *50*, Case No. 15-cv-3312 NC, 2015 WL 13389609, \*2 (N.D. Cal. Sept. 29, 2015). To  
20 determine whether a doe defendant has been identified with sufficient specificity, courts  
21 look to whether a plaintiff provided “the unique IP address[ ] assigned to an individual  
22 defendant on the day of the allegedly infringing conduct” and used “‘geolocation  
23 technology’ to trace the IP addresses to a physical point of origin.” *808 Holdings, LLC v.*  
24 *Collective of Dec. 29, 2011 Sharing Hash*, Case No. 12CV00186 MMA (RBB), 2012 WL  
25 12884688, at \*4 (S.D. Cal. May 8, 2012) (collecting cases) (citing *OpenMind Sols., Inc. v.*  
26 *Does 1-39*, No. C-11-3311 MEJ, 2011 WL 4715200, at \*2 (N.D. Cal. Oct. 7, 2011).  
27 Identifying the unique IP address and location of the IP address has been shown to meet  
28 the requirement for identifying a doe defendant with sufficient specificity. *Id.*

1 Plaintiff has submitted several declarations in support of its request to serve a Rule  
2 45 subpoena: David Williamson, Plaintiff’s Chief Technology Officer; Patrick Paige of  
3 Computer Forensics LLC, retained to analyze forensic evidence captured by Plaintiff’s  
4 infringement detection system; Susan B. Stalzer, an employee of Plaintiff that verifies  
5 infringing files are identical or strikingly similar to Plaintiff’s works; and Emile Kennedy,  
6 Plaintiff’s in-house General Counsel who verifies the infringing IP address traces to San  
7 Diego. (*Ex Parte* Appl, Exs. A (“Williams Decl.”), B (“Paige Decl.”), C (“Stalzer Decl.”),  
8 and D (“Kennedy Decl.”) [ECF 4-2])

9 Here, Plaintiff has identified the Doe Defendant with sufficient specificity. Mr.  
10 Williamson’s declaration explains that he “oversaw the design, development, and overall  
11 creation of the infringement detection system called VXN Scan[,] which [Plaintiff] both  
12 owns and uses to identify the IP addresses used by individuals infringing Plaintiff’s movies  
13 via the BitTorrent protocol.” (Williamson Decl. ¶ 40.) One part of the VXN Scan system  
14 involves the development of a proprietary BitTorrent client that emulates the behavior of a  
15 standard BitTorrent client by repeatedly downloading data pieces from peers within the  
16 BitTorrent network that are distributing Plaintiff’s movies. (*Id.* ¶¶ 52–55.) Mr.  
17 Williamson’s declaration also explains that another component of the VXN Scan system  
18 is the PCAP<sup>1</sup> Recorder that uses a PCAP Capture Card, which can record the IP addresses  
19 connecting to the Proprietary Client and sending the infringed copies of Plaintiff’s work to  
20 the Proprietary Client through the BitTorrent network. (*Id.* ¶¶ 57–59.) A PCAP contains  
21 the IP addresses used in the network transaction, the port number and BitTorrent client  
22 used to accomplish each transaction, and the “Info Hash” associated with the infringing  
23 computer file, which identifies the data that was shared in the recorded transaction as part  
24 of the specific digital media file, *i.e.*, an infringing copy of Plaintiff’s copyrighted works.  
25  
26  
27

---

28 <sup>1</sup> PCAP stands for “Packet Capture.” (Williamson Decl. ¶ 58.)

1 (*Id.* ¶¶ 61–62.) The PCAP Capture Card records perfect copies of every network packet  
2 received by the Proprietary Client. (*Id.* ¶ 65)<sup>2</sup>

3 Mr. Paige’s declaration explains that the VXN Scan recorded numerous BitTorrent  
4 computer transactions with IP address 99.26.121.221 in the form of PCAPs. (Paige Decl.  
5 ¶¶ 13–16.) Mr. Paige then reviewed the PCAP to confirm that it evidences a recorded  
6 transaction with that IP address on September 29, 2020 at 15:16:39 UTC involving the IP  
7 address uploading a piece or pieces of a file corresponding to a specific hash value to VXN  
8 Scan. (*Id.* ¶¶ 16–18.) He then explains that based on his experience in similar cases,  
9 Defendant’s ISP is the only entity that can correlate the identified IP address to its  
10 subscriber to pinpoint Defendant’s identity. (*Id.* ¶ 28.)

11 Ms. Stalzer’s declaration explains that she viewed the unauthorized motion pictures  
12 corresponding with the file hashes side-by-side with Plaintiff’s original movies and verified  
13 that each digital media file obtained from the VXN’s Torrent Collector and Downloader  
14 components is a copy of one of Plaintiff’s copyrighted works. (Stalzer Decl. ¶¶ 10-11.)  
15 Ms. Stalzer then confirmed that ISP AT&T Internet Services did own Defendant’s IP  
16 address at the time of the infringements by using the American Registry for Internet  
17 Numbers. (*Id.* ¶ 12.) And finally, Ms. Kennedy’s declaration explains that she used  
18 Maxmind’s Geolocation Database to trace the infringing IP address to San Diego,  
19 California, within this Court’s jurisdiction, at three different times – when the infringement  
20 data was received from VXN Scan, prior to filing the Complaint, and before submitting  
21 her declaration in support of this motion. (Kennedy Decl. ¶¶ 4-7.) The Court is satisfied  
22 that these multiple geolocation traces indicate that the Defendant is located within this  
23 District.

24 Plaintiff has identified the missing party with such “sufficient specificity” so as to  
25 assure the Court that the Doe Defendant is real, subject to the Court’s jurisdiction, and able  
26

---

27 <sup>2</sup> Mr. Williamson’s declaration sets forth additional in-depth details regarding all  
28 components of the system.

1 to be sued. *Columbia Ins.*, 185 F.R.D. at 578.

2 **B. Previous Steps Taken to Locate Doe Defendant**

3 Plaintiff has sufficiently described all prior attempts it has made to identify Doe  
4 Defendant. *Id.* at 579. This element is aimed at ensuring that “plaintiffs make a good faith  
5 effort to comply with the requirements of service of process and specifically identify  
6 defendants.” *Id.* In addition to the efforts described above to trace the infringing activity  
7 to the IP address, Plaintiff has asserted that it has searched for Doe Defendant’s IP address  
8 “on various web search tools [and] review[ed] numerous sources of authority,” including  
9 technology guides and agency websites, but has not been able to identify Defendant. (*Ex*  
10 *Parte Appl.* at 8.) Further, Plaintiff has “discussed the issue at length with computer  
11 investigators and cyber security consultants [and] does not know how else it could possibly  
12 enforce its copyrights from illegal piracy over the Internet.” (*Id.*) Therefore, the Court  
13 finds that Plaintiff has made a good faith effort to identify the Doe Defendant.

14 **C. Ability to Withstand a Motion to Dismiss**

15 Plaintiff has also demonstrated that its claim could withstand a motion to dismiss.  
16 This requires Plaintiff to “make some showing that an act giving rise to civil liability  
17 actually occurred and that the discovery is aimed at revealing specific identifying features  
18 of the person or entity who committed that act.” *Columbia Ins.*, 185 F.R.D. at 580.

19 A claim may be dismissed pursuant to Rule 12(b) for lack of subject matter  
20 jurisdiction or for failure to state a claim. Fed. R. Civ. P. 12(b)(1), 12 (b)(6). To prevail  
21 on a copyright infringement claim, Plaintiff must show: “(1) ownership of a valid  
22 copyright; and (2) that the defendant violated the copyright owner’s exclusive rights under  
23 the Copyright Act.” *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (citing 17  
24 U.S.C. § 501(a)); *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 666 (9th Cir. 2017).  
25 “Direct infringement requires the plaintiff to show causation (also referred to as ‘volitional  
26 conduct’) by the defendant.” *Perfect 10*, 847 F.3d at 666.

27 Here, Plaintiff’s Complaint alleges subject matter jurisdiction under 28 U.S.C.  
28 § 1331 (federal question) and 28 U.S.C. § 1338 (jurisdiction over copyright actions).

1 (Compl. ¶ 7.) Further, Plaintiff provides evidence that it is the exclusive rights holder of  
2 the copyrighted works at issue. (See Compl., Ex. A.)<sup>3</sup> Plaintiff alleges that Defendant  
3 infringed Plaintiff’s copyrighted work via the BitTorrent file distribution network. (Compl.  
4 ¶¶ 41-46, Ex. A.) Plaintiff also alleges that it did not permit or consent to Doe Defendant’s  
5 copying or distribution of this work. (Id. ¶ 51.) Accordingly, Plaintiff has alleged the  
6 prima facie elements of direct copyright infringement and could withstand a motion to  
7 dismiss for failure to state a claim. See *Columbia Ins.*, 185 F.R.D. at 579-80. Additionally,  
8 the Court finds the Complaint could withstand a challenge based on personal jurisdiction  
9 or venue. As discussed at length above, Plaintiff has traced the infringing conduct to this  
10 district. (III.A.)

11 **D. Requested Discovery Will Lead to Identifying Information**

12 Finally, Plaintiff has satisfied the last element required in *Columbia Insurance* by  
13 demonstrating the requested discovery will lead to identifying information about Doe  
14 Defendant that would make service of process possible. *Columbia Ins.*, 185 F.R.D. at 580.  
15 As explained above, Plaintiff’s investigation has revealed a unique IP address. Due to the  
16 fact that the only entity able to correlate an IP address to a specific individual is the ISP,  
17 AT&T U-Verse, the requested Rule 45 subpoena would lead to information making  
18 physical service of process possible.

19 **IV. CONCLUSION AND ORDER**

20 The *Ex Parte* Application (ECF No. 4) is **GRANTED**. Accordingly, **IT IS**  
21 **HEREBY ORDERED** that:

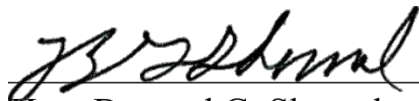
- 22 1. Plaintiff may serve AT&T U-Verse with a Rule 45 subpoena commanding the  
23 ISP to provide Plaintiff with the true name and address of the subscriber assigned  
24 \_\_\_\_\_

25  
26 <sup>3</sup> Exhibit A is a chart containing United States Copyright Office registration information,  
27 including the registration numbers and application numbers for those works who  
28 registration is still pending. In its Complaint, Plaintiff states that it “owns the copyrights to  
the Works and the Works have either been registered with the United States Copyright  
Office or have pending copyright registrations.” (Compl. ¶¶ 42-46.)

1 the IP address 99.26.121.221. Plaintiff may not subpoena additional information  
2 about the subscriber and Plaintiff may only use the disclosed information to  
3 protect its copyrights in pursuing this litigation.

- 4 2. Plaintiff shall attach a copy of this Order to any Rule 45 subpoena issued pursuant  
5 to this Order and the ISP must also provide a copy of this Order along with the  
6 required notice to the subscriber whose identity is sought.
- 7 3. Within **fourteen (14) calendar days** after the service of the subpoena, the ISP  
8 shall notify the subscriber that its identity has been subpoenaed by Plaintiff.
- 9 4. The subscriber whose identity has been subpoenaed shall have **thirty (30)**  
10 **calendar days** from the date of such notice to seek a protective order or challenge  
11 the disclosure by filing an appropriate pleading with this Court contesting the  
12 subpoena. The subscriber may proceed anonymously as a Doe Defendant until  
13 the Court orders otherwise.<sup>4</sup>
- 14 5. If the ISP wishes to move to quash the subpoena, it shall do so before the return  
15 date of the subpoena. The return date of the subpoena must allow for **forty-five**  
16 **(45) calendar days** from service to production. If a motion to quash or other  
17 customer challenge is brought, the ISP shall preserve the information sought by  
18 Plaintiff in the subpoena pending resolution of such motion or challenge.

19  
20 Dated: February 5, 2021

21   
22 Hon. Bernard G. Skomal  
23 United States Magistrate Judge  
24  
25  
26

27  
28 <sup>4</sup> Plaintiff's *Ex Parte* Application specifically states that Plaintiff is not opposed and "in fact welcomes" allowing Defendant to proceed anonymously. (*Ex Parte* Appl. at 12.)