

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

11 STRIKE 3 HOLDINGS, LLC,  
12 Plaintiff,  
13 v.  
14 JOHN DOE, Subscriber Assigned IP  
15 Address 72.199.88.168,  
16 Defendant.

Case No.: 23-cv-00942-RSH-JLB

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

[ECF No. 4]

17  
18 Before the Court is an *Ex Parte* Application for Leave to Serve a Third-Party  
19 Subpoena Prior to a Rule 26(f) Conference (“Motion”) filed by Plaintiff Strike 3 Holdings,  
20 LLC (“Plaintiff”). (ECF No. 4.) No opposition has been filed, as no defendant has been  
21 named or served in this case. For the reasons set forth below, Plaintiff’s *ex parte* Motion  
22 is **GRANTED**.

23 **I. BACKGROUND**

24 This is one of the numerous cases filed by Plaintiff alleging copyright infringement  
25 claims against a John Doe defendant using the BitTorrent file-sharing system.<sup>1</sup> Plaintiff  
26

27  
28 <sup>1</sup> From January 2020 to date, Strike 3 Holdings, LLC, has filed over one hundred cases, including this one, in this District.

1 alleges that it is the copyright owner of motion pictures distributed through adult content  
2 websites *Blacked*, *Tushy*, *Tushy Raw*, *Vixen*, *Blacked Raw*, and *Slayed*. (ECF No. 1 ¶¶ 2–  
3 3.) Plaintiff alleges that between October 29, 2022, and May 8, 2023,<sup>2</sup> the person or entity  
4 assigned Internet Protocol (“IP”) address 72.199.88.168 illegally downloaded and  
5 distributed twenty-four of Plaintiff’s motion pictures through his, her, or its use of the  
6 online BitTorrent file distribution network. (*Id.* ¶¶ 4–5, 18–42; ECF No. 1-2.) Plaintiff  
7 commenced this action against Defendant “John Doe, subscriber assigned IP address  
8 72.199.88.168” on May 22, 2023, alleging a single cause of action of direct copyright  
9 infringement. (ECF No. 1 ¶¶ 48–53.)

10 Because Defendant used the Internet to commit the alleged infringement, Plaintiff  
11 alleges that it knows Defendant only by his, her, or its IP address, which was assigned to  
12 Defendant by the Internet Service Provider (“ISP”), Cox Communications. (*Id.* ¶¶ 5, 13.)  
13 In the instant Motion, Plaintiff asserts that Cox Communications is the owner of  
14 Defendant’s IP address, and thus, “is the only party with the information necessary to  
15 identify Defendant by correlating the IP address with John Doe’s identity.” (ECF No. 4-1  
16 at 7.) Plaintiff therefore seeks leave to serve a Rule 45 subpoena on Cox Communications  
17 requesting the true name and address associated with IP address 72.199.88.168. (*Id.* at 7–  
18 8.) Without Defendant’s identity, Plaintiff cannot serve Defendant and prosecute this case.  
19 (*Id.* at 8.)

## 20 **II. LEGAL STANDARD**

21 Discovery is not permitted before the parties have conferred pursuant to Federal Rule  
22 of Civil Procedure 26(f) unless authorized by court order. Fed. R. Civ. P. 26(d)(1).  
23 “[H]owever, in rare cases, courts have made exceptions, permitting limited discovery to  
24

---

25  
26 <sup>2</sup> Plaintiff does not specifically allege this infringement period in the Complaint.  
27 However, attached as an exhibit to the Complaint is a table reflecting that the subscriber  
28 assigned IP address 72.199.88.168 engaged in allegedly infringing activity between  
June 25, 2022, and May 8, 2023. (ECF No. 1-2.)

1 ensue after filing of the complaint to permit the plaintiff to learn the identifying facts  
2 necessary to permit service on the defendant.” *Columbia Ins. Co. v. Seescandy.com*, 185  
3 F.R.D. 573, 577 (N.D. Cal. 1999). Requests to conduct discovery prior to a Rule 26(f)  
4 conference are granted upon a showing of good cause by the moving party, which may be  
5 found “where the need for expedited discovery, in consideration of the administration of  
6 justice, outweighs the prejudice to the responding party.” *Semitoool, Inc. v. Tokyo Electron*  
7 *Am., Inc.*, 208 F.R.D. 273, 275–76 (N.D. Cal. 2002). “A district court’s decision to grant  
8 discovery to determine jurisdictional facts is a matter of discretion.” *Columbia Ins. Co.*,  
9 185 F.R.D. at 578.

10 District courts in the Ninth Circuit apply a three-factor test to determine whether  
11 good cause exists to allow for expedited discovery to identify a Doe defendant. *Id.* at 578–  
12 80. “First, the plaintiff should identify the missing party with sufficient specificity such  
13 that the Court can determine that [the] defendant is a real person or entity who could be  
14 sued in federal court.” *Id.* at 578. Second, the plaintiff “should identify all previous steps  
15 taken to locate the elusive defendant” to ensure that the plaintiff has made a good faith  
16 effort to identify and serve process on the defendant. *Id.* at 579. Third, the plaintiff “should  
17 establish to the Court’s satisfaction that [the] plaintiff’s suit against [the] defendant could  
18 withstand a motion to dismiss.” *Id.* “Lastly, the plaintiff should file a request for discovery  
19 with the Court, along with a statement of reasons justifying the specific discovery requested  
20 as well as identification of a limited number of persons or entities on whom discovery  
21 process might be served and for which there is a reasonable likelihood that the discovery  
22 process will lead to identifying information about [the] defendant that would make service  
23 of process possible.” *Id.* at 580.

### 24 **III. DISCUSSION**

#### 25 **A. Identification of Missing Party with Sufficient Specificity**

26 For the Court to grant Plaintiff’s Motion, Plaintiff must first identify Defendant with  
27 enough specificity to enable the Court to determine that Defendant is a real person or entity  
28

1 who is subject to the Court’s jurisdiction. *See Columbia Ins. Co.*, 185 F.R.D. at 578. The  
2 Court finds that Plaintiff has met this burden.

3 Courts in the Ninth Circuit have determined that “a plaintiff identifies Doe  
4 defendants with sufficient specificity” in cases like the instant case “by providing the  
5 unique IP addresses assigned to an individual defendant on the day of the allegedly  
6 infringing conduct, and by using ‘geolocation technology’ to trace the IP addresses to a  
7 physical point of origin.” *808 Holdings, LLC v. Collective of December 29, 2011 Sharing*  
8 *Hash E37917C8EEB4585E6421358FF32F29C D63C23C91*, No. 12-cv-00186-MMA-  
9 RBB, 2012 WL 12884688, at \*4 (S.D. Cal. May 8, 2012); *see also Pink Lotus Entm’t, LLC*  
10 *v. Does 1–46*, No. C-11-02263, 2011 WL 2470986, at \*3 (N.D. Cal. June 21, 2011) (finding  
11 that the plaintiff met its burden to identify the Doe defendants with sufficient specificity  
12 by identifying the Doe defendants’ IP addresses and then using geolocation technology to  
13 trace the IP addresses to a point of origin).

14 Here, Plaintiff has sufficiently demonstrated that Defendant is a real person or entity  
15 likely subject to the Court’s jurisdiction. Plaintiff attached to its Complaint a table  
16 reflecting that the subscriber assigned IP address 72.199.88.168 engaged in allegedly  
17 infringing activity between October 29, 2022, and May 8, 2023, in San Diego, California.  
18 (ECF No. 1-2.) To substantiate these claims, Plaintiff attached four declarations to the  
19 instant Motion.

20 Plaintiff first attached the Declaration of David Williamson, an independent  
21 contractor hired by Plaintiff as an Information Systems and Management Consultant.  
22 (ECF No. 4-2 at 1–15 (“Ex. A”).) Mr. Williamson states that he “oversaw the design,  
23 development, and overall creation of the infringement detection system called VXN Scan[,]  
24 which [Plaintiff] both owns and uses to identify the IP addresses used by individuals  
25 infringing Plaintiff’s movies via the BitTorrent protocol.” (Ex. A ¶ 40.) Mr. Williamson’s  
26 declaration explains in detail how VXN Scan operates and its six components. One  
27 component of VXN Scan is a proprietary BitTorrent client that emulates the behavior of a  
28 standard BitTorrent client by repeatedly downloading data pieces from peers within the

1 BitTorrent network that are distributing Plaintiff’s movies. (*Id.* ¶¶ 52–56.) Another  
2 component of VXN Scan is the PCAP Recorder, which records infringing BitTorrent  
3 computer transactions in the form of PCAPs, or packet captures. (*Id.* ¶¶ 57–70.) The  
4 PCAPs contain the IP addresses that connect to the Proprietary Client and send pieces of  
5 the computer file containing an infringing copy of one of Plaintiff’s movies to the  
6 Proprietary Client through the BitTorrent network. (*Id.* ¶¶ 57–59.) Not only do PCAPs  
7 record the IP addresses used in the network transaction, but they also record the date and  
8 time of the transaction, the port number used, and the BitTorrent client used to accomplish  
9 each transaction. (*Id.* ¶ 61.) PCAPs also identify the “Info Hash value that was used to  
10 obtain the transacted piece.” (*Id.* ¶ 62.) This information identifies the data that was shared  
11 in the recorded transaction as part of a file containing an infringing copy of one of  
12 Plaintiff’s movies. (*Id.*) This Order touches on only two of the components of VXN Scan,  
13 but Mr. Williamson’s eighty-one-paragraph declaration sets forth additional, in-depth  
14 details of all six components of the system, providing the Court with a thorough  
15 understanding of how the system reliably identifies the IP addresses assigned to individuals  
16 infringing Plaintiff’s movies and verifies the infringement. (*See id.* ¶¶ 43–51, 63–81.)

17         Second, Plaintiff attached the Declaration of Patrick Paige, a computer forensics  
18 expert Plaintiff retained to analyze and retain evidence captured by VXN Scan.  
19 (ECF No. 4-2 at 16–22 (“Ex. B”).) Mr. Paige explains that VXN Scan “recorded numerous  
20 BitTorrent computer transactions between the system and IP address 72.199.88.168 in the  
21 form of PCAPs.” (Ex. B ¶ 13.) Mr. Paige states that, using a program called Wireshark,  
22 he viewed and analyzed a PCAP he received from Plaintiff and was able to confirm that on  
23 May 08, 2023, “IP address 72.199.88.168 uploaded a piece or pieces of a file corresponding  
24 to hash value F6D6E795148593F639DC8362628B2C02D1F474CA to VXN Scan.”  
25 (*Id.* ¶¶ 16–19.) The hash value, or Info Hash, is the data used by BitTorrent to identify and  
26 locate other pieces of a desired file; in this case, the desired file contained an infringing  
27 copy of one of Plaintiff’s movies. (*Id.* ¶ 22; *see also* ECF No. 1-2 at 1.) Based on his  
28 experience in similar cases, Mr. Paige opines that Cox Communications, Defendant’s ISP,

1 “is the only entity that can correlate the IP address [72.199.88.168] to its subscriber and  
2 identify Defendant as the person assigned [this] IP address . . . during the time of the alleged  
3 infringement.” (*Id.* ¶ 28.)

4 Third, Plaintiff attached the Declaration of Susan B. Stalzer, an employee of  
5 Plaintiff’s who verified that each digital file VXN Scan received through its transactions  
6 with IP address 72.199.88.168 was identical, strikingly similar, or substantially similar to  
7 one of Plaintiff’s original copyrighted works. (ECF No. 4-2 at 23–26 (“Ex. C”).) To do  
8 so, Ms. Stalzer viewed each of the digital media files side-by-side with Plaintiff’s original  
9 films. (Ex. C ¶¶ 8–10.)

10 Last, Plaintiff attached the Declaration of Emilie Kennedy, Plaintiff’s in-house  
11 General Counsel. (ECF No. 4-2 at 27–30 (“Ex. D”).) Ms. Kennedy explains that after  
12 Plaintiff received data from VXN Scan identifying IP address 72.199.88.168 as infringing  
13 its movies, “the IP address was automatically inputted into Maxmind’s Geolocation  
14 Database” on May 18, 2023.<sup>3</sup> (Ex. D ¶ 4.) “Maxmind [then] determined that the IP address  
15 traced to a location in San Diego, California, which is within this Court’s jurisdiction.”  
16 (*Id.* ¶ 5.) Ms. Kennedy states that Plaintiff inputted IP address 72.199.88.168 again into  
17 the Maxmind Database “[p]rior to filing its Complaint” and “before filing [her]

---

18  
19  
20 <sup>3</sup> Mr. Williamson provides in his declaration that:

21 Maxmind is “an industry-leading provider of IP intelligence and  
22 online fraud detection tools.” “Over 5,000 companies use GeoIP  
23 data to locate their Internet visitors and show them relevant  
24 content and ads, perform analytics, enforce digital rights, and  
25 efficiently route Internet traffic.” Maxmind is not “software” or  
26 technology, but . . . a database. Maxmind compiles information  
27 it receives from Internet Service Providers (ISPs) containing the  
28 city and state locations of the users of the ISPs and their  
respective IP addresses. Maxmind maintains and updates this list  
weekly and sells access to it.

(Ex. A ¶ 77 (footnotes omitted).)

1 [D]eclaration,” and both times the IP address “continued to trace to this District.” (*Id.* ¶ 6–  
2 7.) In its Motion, Plaintiff argues that this Court has previously “accepted Maxmind’s  
3 findings for purposes of allowing expedited discovery.” (ECF No. 4-1 at 13 (citing *Strike*  
4 *3 Holdings, LLC v. Doe*, No. CV 17-2317-JAH (BLM), 2017 WL 6389848, at \*2 (S.D.  
5 Cal. Dec. 14, 2017)).)

6 Based on Plaintiff’s IP address tracing efforts, the timing of its efforts, and Plaintiff’s  
7 continued tracing of IP address 72.199.88.168 to a location within San Diego, California,  
8 the Court concludes that Plaintiff has met its evidentiary burden of identifying Defendant  
9 with sufficient specificity and has shown that Defendant’s IP address likely relates to a  
10 physical address within the Court’s jurisdiction.

#### 11 **B. Previous Attempts to Locate Defendant**

12 Plaintiff must next identify all steps it took to locate Defendant to ensure the Court  
13 that it has made a good-faith effort to identify and serve process on Defendant.  
14 *See Columbia Ins. Co.*, 185 F.R.D. at 579. The Court finds that Plaintiff has met this  
15 burden.

16 In its Motion, Plaintiff states that it has diligently attempted to locate Defendant by  
17 searching for Defendant’s IP address using online search engines and “various web search  
18 tools.” (ECF No. 4-1 at 14.) Plaintiff has also “review[ed] numerous sources of authority,”  
19 such as “legislative reports, agency websites, informational technology guides, [and]  
20 governing case law” regarding whether it is possible to identify such a defendant by other  
21 means and has “discussed the issue at length with computer investigators and cyber security  
22 consultants.” (*Id.*) Plaintiff argues that it cannot determine any other means of obtaining  
23 Defendant’s identity other than through subpoenaing the information from Defendant’s  
24 ISP, as it has “exhausted all other alternatives for identifying Defendant.” (*Id.*)

25 Further, as discussed above, Plaintiff retained Mr. Paige, a computer forensics  
26 expert, who analyzed the data captured by VXN Scan and was able to determine that IP  
27 address 72.199.88.168 was engaged in the allegedly infringing activity on May 8, 2023.  
28 (*See Ex. B* ¶¶ 13–26.) Mr. Paige also opined that Defendant’s ISP is the only entity that

1 can correlate IP address 72.199.88.168 to its subscriber and identify Defendant as the  
2 person assigned this IP address during the time of the alleged infringement. (*Id.* ¶ 28.)

3 Based on the foregoing, the Court is satisfied that Plaintiff has attempted in good  
4 faith to locate Defendant and that Plaintiff cannot, on its own, identify Defendant with any  
5 greater specificity than as the subscriber assigned by Cox Communications to IP address  
6 72.199.88.168. Accordingly, the Court finds that Plaintiff has made a good-faith effort to  
7 identify and locate Defendant before filing the instant Motion.

### 8 **C. Whether Plaintiff’s Complaint Could Withstand a Motion to Dismiss**

9 Lastly, Plaintiff must establish that its Complaint could survive a motion to dismiss.  
10 *Columbia Ins. Co.*, 185 F.R.D. at 579. The Court finds that Plaintiff has met this burden.

11 Plaintiff’s Complaint alleges a single cause of action against Defendant: direct  
12 copyright infringement. (ECF No. 1 ¶¶ 48–53.) To survive a motion to dismiss for failure  
13 to state a claim upon which relief can be granted, “a complaint must contain sufficient  
14 factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’”  
15 *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S.  
16 544, 570 (2007)). To state a claim of direct copyright infringement, a plaintiff “must  
17 show: (1) ownership of a valid copyright; and (2) that the defendant violated the copyright  
18 owner’s exclusive rights under the Copyright Act.” *Ellison v. Robertson*, 357 F.3d 1072,  
19 1076 (9th Cir. 2004) (citing 17 U.S.C. § 501(a) (2003)). “In addition, direct infringement  
20 requires the plaintiff to show causation (also referred to as ‘volitional conduct’) by the  
21 defendant.” *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 666 (9th Cir. 2017).

22 In the Complaint, Plaintiff alleges to be the owner of the copyrighted movies or  
23 “[w]orks” at issue and asserts that each work was registered with the United States  
24 Copyright Office. (ECF No. 1 ¶¶ 2, 46.) Exhibit A to the Complaint shows the hash values  
25 of the purportedly infringed works and the copyright registration number for each of the  
26 works that correspond with those hash values. (ECF No. 1-2.) Plaintiff further alleges that  
27 Defendant is the user behind IP address 72.199.88.168 who used the BitTorrent file  
28 network to “illegally download and distribute Plaintiff’s copyrighted motion pictures” and



1 that the infringement was “continuous and ongoing.” (ECF No. 1 ¶¶ 13, 29, 45.) Lastly,  
2 Plaintiff alleges that “[a]t no point in time did [it] authorize, permit or consent to  
3 Defendant’s copying, distribution, performance and/or display of its Works, expressly or  
4 otherwise.” (*Id.* ¶ 51.)

5 The Court finds that Plaintiff has alleged a prima facie case of direct copyright  
6 infringement and therefore, its Complaint would likely withstand a motion to dismiss by  
7 Defendant.

#### 8 **D. Specific Discovery Request**

9 Finally, before the Court grants Plaintiff’s Motion, Plaintiff “should file a request  
10 for discovery with the Court.” *Columbia Ins. Co.*, 185 F.R.D. at 580. Plaintiff has not  
11 provided the Court with a proposed subpoena, but the Court has sufficient information to  
12 determine that “there is a reasonable likelihood that [a subpoena] will lead to identifying  
13 information about [D]efendant that would make service of process possible.” *Id.* Plaintiff  
14 states that it plans to issue a subpoena upon Cox Communications, Defendant’s ISP,  
15 requesting “only the true name and address” of Defendant, the subscriber of IP address  
16 72.199.88.168. (ECF No. 4-1 at 7–8.) Further, Plaintiff provides that Cox  
17 Communications is the only entity that can identify Defendant by his, her, or its IP address.  
18 (Ex. B ¶ 28.) Accordingly, the Court finds that Plaintiff need not file the proposed  
19 subpoena with the Court.

#### 20 **IV. CONCLUSION**

21 For the reasons set forth above, the Court finds good cause to grant Plaintiff leave to  
22 serve a Rule 45 subpoena upon Cox Communications in advance of the Rule 26(f)  
23 conference. However, despite Plaintiff’s representations of good faith (ECF No. 4-1 at 9–  
24 10), the Court shares the concern noted by other courts in this District of “unscrupulous  
25 tactics [being] used by certain plaintiffs, especially in the adult film industry, to shake down  
26 the owners of IP addresses’ to exact quick and quiet settlements from possibly innocent  
27 defendants who pay out only to avoid potential embarrassment.” *Malibu Media, LLC v.*  
28 *Doe*, No. 16-cv-00786-JLS-NLS, 2016 WL 9488778, at \*4 (S.D. Cal. May 6, 2016)

1 (quoting *Malibu Media, LLC v. Does 1–5*, No. 12 Civ. 2950(JPO), 2012 WL 2001968, at  
2 \*1 (S.D.N.Y. June 1, 2012)). The Court therefore finds that a limited protective order is  
3 necessary to protect Defendant’s privacy. Further, Plaintiff has invited the Court to issue  
4 a protective order establishing procedural safeguards, “should the Court find such  
5 procedures to be appropriate.” (ECF No. 4-1 at 18.) Accordingly, the Court **GRANTS**  
6 Plaintiff’s *ex parte* Motion (ECF No. 4) and **ORDERS** as follows:

7 1. Plaintiff may serve on Cox Communications a subpoena, pursuant to and  
8 compliant with the procedures of Federal Rule of Civil Procedure 45, seeking only the  
9 name and address of the subscriber assigned IP address 72.199.88.168 for the relevant time  
10 period of the alleged infringement. Plaintiff shall not seek from Cox Communications any  
11 other personally identifiable information about the subscriber.

12 2. Plaintiff’s subpoena to Cox Communications must provide a minimum of  
13 forty-five (45) calendar days’ notice before any production responsive to the subpoena  
14 shall be made to Plaintiff.

15 3. At the time Plaintiff serves its subpoena on Cox Communications, Plaintiff  
16 shall also serve on Cox Communications a copy of this Order.

17 4. Within fourteen (14) calendar days after service of the subpoena, Cox  
18 Communications shall notify the subscriber assigned IP address 72.199.88.168 that his,  
19 her, or its identity has been subpoenaed by Plaintiff and shall provide the subscriber a copy  
20 of this Order with the required notice.

21 5. The subscriber whose identity has been subpoenaed shall have thirty (30)  
22 calendar days from the date of such notice to challenge Cox Communications’s disclosure  
23 of his, her, or its name and address by filing an appropriate pleading with this Court  
24 contesting the subpoena.

25 6. If Cox Communications seeks to modify or quash the subpoena, it shall do so  
26 as provided by Federal Rule of Civil Procedure 45(d)(3).

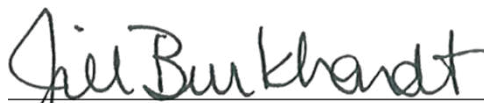
27 ///  
28 ///

1           7.     In the event a motion to quash, modify, or otherwise challenge the subpoena  
2 is brought properly before the Court, Cox Communications shall preserve the information  
3 sought by the subpoena pending the resolution of any such motion.

4           8.     Plaintiff may only use the information disclosed in response to a Rule 45  
5 subpoena served on Cox Communications for the purpose of protecting and enforcing  
6 Plaintiff's rights as set forth in the Complaint (ECF No. 1). If Defendant wishes to proceed  
7 anonymously, Plaintiff may not release any identifying information without a court order  
8 allowing the release of the information.

9           **IT IS SO ORDERED.**

10          Dated: July 7, 2023

  
\_\_\_\_\_  
Hon. Jill L. Burkhardt  
United States Magistrate Judge

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28