

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 23.119.229.181,

Defendant.

Case No.: 22-cv-01363-TWR-JLB

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

[ECF No. 3]

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

I. BACKGROUND

This is one of the numerous cases filed by Plaintiff alleging copyright infringement claims against a John Doe defendant using the BitTorrent file-sharing system.¹ Plaintiff

¹ 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*, *Vixen*, and *Blacked Raw*. (ECF No. 1 ¶¶ 3–4.) Plaintiff alleges
3 that between May 25, 2022, and August 24, 2022,² the person or entity assigned Internet
4 Protocol (“IP”) address 23.119.229.181 illegally downloaded and distributed twenty-eight
5 of Plaintiff’s motion pictures through his, her, or its use of the online BitTorrent file
6 distribution network. (*Id.* ¶¶ 4, 5, 18–42; ECF No. 1-2.) Plaintiff commenced this action
7 against Defendant “John Doe, subscriber assigned IP address 23.119.229.181” on
8 September 9, 2022, alleging a single cause of action of direct copyright infringement.
9 (ECF No. 1 ¶¶ 5, 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”), AT&T U-verse. (*Id.* ¶¶ 5, 13.) In the
13 instant motion, Plaintiff asserts that AT&T U-verse is the owner of Defendant’s IP address,
14 and thus, “is the only party with the information necessary to identify Defendant.”
15 (ECF No. 3-1 at 7.) Plaintiff therefore seeks leave to serve a Rule 45 subpoena on AT&T
16 U-verse requesting the true name and address associated with IP address 23.119.229.181.
17 (*Id.* at 8.) Without Defendant’s identity, Plaintiff cannot serve Defendant and prosecute
18 this case. (*Id.*)

19 **II. LEGAL STANDARD**

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

25
26 ² 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 23.119.229.181 engaged in allegedly infringing activity between
May 25, 2022 and August 24, 2022. (ECF No. 1-2.)

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

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

23 **III. DISCUSSION**

24 **A. Identification of Missing Party with Sufficient Specificity**

25 For the Court to grant Plaintiff’s motion, Plaintiff must first identify Defendant with
26 enough specificity to enable the Court to determine that Defendant is a real person or entity
27 who is subject to the Court’s jurisdiction. *See Columbia Ins. Co.*, 185 F.R.D. at 578. The
28 Court finds that Plaintiff has met this burden.

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

12 Here, Plaintiff has sufficiently demonstrated that Defendant is a real person or entity
13 likely subject to the Court’s jurisdiction. Plaintiff attached to its Complaint a table
14 reflecting that the subscriber assigned IP address 23.119.229.181 engaged in allegedly
15 infringing activity between May 25, 2022, and August 24, 2022, in San Diego, California.
16 (ECF No. 1-2.) To substantiate these claims, Plaintiff attached four declarations to the
17 instant motion.

18 Plaintiff first attached the Declaration of David Williamson, an independent
19 contractor hired by Plaintiff as an Information Systems and Management Consultant.
20 (ECF No. 3-2 at 1–15 (“Ex. A”).) Mr. Williamson states that he “oversaw the design,
21 development, and overall creation of the infringement detection system called VXN Scan[,]
22 which [Plaintiff] both owns and uses to identify the IP addresses used by individuals
23 infringing Plaintiff’s movies via the BitTorrent protocol.” (Ex. A ¶ 40.) Mr. Williamson’s
24 declaration explains in detail how VXN Scan operates and its six components. One
25 component of VXN Scan is a proprietary BitTorrent client that emulates the behavior of a
26 standard BitTorrent client by repeatedly downloading data pieces from peers within the
27 BitTorrent network that are distributing Plaintiff’s movies. (*Id.* ¶¶ 52–55.) Another
28 component of VXN Scan is the PCAP Recorder, which records infringing BitTorrent

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

15 Second, Plaintiff attached the Declaration of Patrick Paige, a computer forensics
16 expert Plaintiff retained to analyze and retain evidence captured by VXN Scan.
17 (ECF No. 3-2 at 16–22 (“Ex. B”).) Mr. Paige explains that VXN Scan “recorded numerous
18 BitTorrent computer transactions between the system and IP address 23.119.229.181.1 in
19 the form of PCAPs.” (Ex. B ¶ 13.) Mr. Paige states that, using a program called Wireshark,
20 he viewed and analyzed a PCAP he received from Plaintiff and was able to confirm that on
21 August 24, 2022, “IP address 23.119.229.181 uploaded a piece or pieces of a file
22 corresponding to hash value 42920509D6F4FE3676865E34D5507154D6A0F712 to VXN
23 Scan.” (*Id.* ¶¶ 16–19.) The hash value, or Info Hash, is the data used by BitTorrent to
24 identify and locate other pieces of a desired file; in this case, the desired file contained an
25 infringing copy of one of Plaintiff’s movies. (*Id.* ¶ 22; *see also* ECF No. 1-2 at 1.) Based
26 on his experience in similar cases, Mr. Paige opines that AT&T U-verse, Defendant’s ISP,
27 “is the only entity that can correlate the IP address [23.119.229.181] to its subscriber and
28

1 identify Defendant as the person assigned [this] IP address . . . during the time of the alleged
2 infringement.” (*Id.* ¶ 28.)

3 Third, Plaintiff attached the Declaration of Susan B. Stalzer, an employee of
4 Plaintiff’s who verified that each digital file VXN Scan received through its transactions
5 with IP address 23.119.229.181 was identical, strikingly similar, or substantially similar to
6 one of Plaintiff’s original copyrighted works. (ECF No. 3-2 at 23–26 (“Ex. C”).) To do
7 so, Ms. Stalzer viewed each of the digital media files side-by-side with Plaintiff’s original
8 films. (Ex. C ¶¶ 8–10.)

9 Last, Plaintiff attached the Declaration of Emilie Kennedy, Plaintiff’s in-house
10 General Counsel. (ECF No. 3-2 at 27–30 (“Ex. D”).) Ms. Kennedy explains that after
11 Plaintiff received data from VXN Scan identifying IP address 23.119.229.181 as infringing
12 its movies, “the IP address was automatically inputted into Maxmind’s Geolocation
13 Database” on September 1, 2022.³ (Ex. D ¶ 4.) “Maxmind [then] determined that the IP
14 address traced to a location in San Diego, California, which is within this Court’s
15 jurisdiction.” (*Id.* ¶ 5.) Ms. Kennedy states that Plaintiff inputted IP address
16 23.119.229.181 again into the Maxmind Database “[p]rior to filing its Complaint” and
17 “before filing [her] [D]eclaration” on September 20, 2022, and both times the IP address
18 traced to San Diego, California. (*Id.* ¶¶ 6–7.) In its motion, Plaintiff argues that this Court
19

20
21 ³ Mr. Williamson provides in his declaration that:

22 Maxmind is “an industry-leading provider of IP intelligence and online fraud
23 detection tools.” “Over 5,000 companies use GeoIP data to locate their
24 Internet visitors and show them relevant content and ads, perform analytics,
25 enforce digital rights, and efficiently route Internet traffic.” Maxmind is not
26 “software” or technology, but . . . a database. Maxmind compiles information
27 it receives from Internet Service Providers (ISPs) containing the city and state
28 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 has previously “accepted Maxmind’s findings for purposes of allowing expedited
2 discovery,” citing, *inter alia*, *Crim. Prods., Inc. v. Doe-72.192.163.220*, No. 16-CV-2589
3 WQH (JLB), 2016 WL 6822186, at *3 (S.D. Cal. Nov. 18, 2016). (ECF No. 3-1 at 13.)

4 Based on Plaintiff’s IP address tracing efforts, the timing of its efforts, and Plaintiff’s
5 continued tracing of IP address 23.119.229.181 to a location within San Diego, California,
6 the Court concludes that Plaintiff has met its evidentiary burden of identifying Defendant
7 with sufficient specificity and has shown that Defendant’s IP address likely relates to a
8 physical address within the Court’s jurisdiction.

9 **B. Previous Attempts to Locate Defendant**

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

14 In its motion, Plaintiff states that it has diligently attempted to locate Defendant by
15 searching for Defendant’s IP address using online search engines and “various web search
16 tools.” (ECF No. 3-1 at 14.) Plaintiff has also “review[ed] numerous sources of authority,”
17 such as “legislative reports, agency websites, informational technology guides, [and]
18 governing case law” regarding whether it is possible to identify such a defendant by other
19 means and has “discussed the issue at length with computer investigators and cyber security
20 consultants.” (*Id.*) Plaintiff argues that it cannot determine any other means of obtaining
21 Defendant’s identity other than through subpoenaing the information from Defendant’s
22 ISP, as it has “exhausted all other alternatives for identifying Defendant.” (*Id.*)

23 Further, as discussed above, Plaintiff retained Mr. Paige, a computer forensics
24 expert, who analyzed the data captured by VXN Scan and was able to determine that IP
25 address 23.119.229.181 was engaged in the allegedly infringing activity on
26 August 24, 2022. (*See* Ex. B ¶¶ 13–26.) Mr. Paige also opined that Defendant’s ISP is the
27 only entity that can correlate IP address 23.119.229.181 to its subscriber and identify
28 Defendant as the person assigned this IP address during the time of the alleged

1 infringement. (*Id.* ¶ 28.)

2 Based on the foregoing, the Court is satisfied that Plaintiff has attempted in good
3 faith to locate Defendant and that Plaintiff cannot, on its own, identify Defendant with any
4 greater specificity than as the subscriber assigned by AT&T U-verse to IP address
5 23.119.229.181. Accordingly, the Court finds that Plaintiff has made a good-faith effort
6 to identify and locate Defendant before filing the instant motion.

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

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

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

21 In the Complaint, Plaintiff alleges to be the owner of the copyrighted movies or
22 “works” at issue and asserts that each work was registered with the United States Copyright
23 Office. (ECF No. 1 ¶¶ 2, 46.) Exhibit A to the Complaint shows the hash values of the
24 purportedly infringed works and the copyright registration number for each of the works
25 that correspond with those hash values. (ECF No. 1-2.) Plaintiff further alleges that
26 Defendant is the user behind IP address 23.119.229.181 who used the BitTorrent file
27 network to “illegally download and distribute Plaintiff’s copyrighted motion pictures” and
28 that the infringement was “continuous and ongoing.” (ECF No. 1 ¶¶ 13, 29, 45.) Lastly,

1 Plaintiff alleges that “[a]t no point in time did [it] authorize, permit or consent to
2 Defendant’s copying, distribution, performance and/or display of its Works, expressly or
3 otherwise.” (*Id.* ¶ 51.)

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

7 **D. Specific Discovery Request**

8 Finally, before the Court grants Plaintiff’s Motion, Plaintiff “should file a request
9 for discovery with the Court.” *Columbia Ins. Co.*, 185 F.R.D. at 580. Plaintiff has not
10 provided the Court with a proposed subpoena, but the Court has sufficient information to
11 determine that “there is a reasonable likelihood that [a subpoena] will lead to identifying
12 information about [D]efendant that would make service of process possible.” *Id.* Plaintiff
13 states that it plans to issue a subpoena upon AT&T U-verse, Defendant’s ISP, requesting
14 “the true name and address” of Defendant, the subscriber of IP address 23.119.229.181.
15 (ECF No. 3-1 at 8.) Further, Plaintiff provides that AT&T U-verse is the only entity that
16 can identify Defendant by his, her, or its IP address. (Ex. B ¶ 28.) Accordingly, the Court
17 finds that Plaintiff need not file the proposed subpoena with the Court.

18 **IV. CONCLUSION**

19 For the reasons set forth above, the Court finds good cause to grant Plaintiff leave to
20 serve a Rule 45 subpoena upon AT&T U-verse in advance of the Rule 26(f) conference.
21 However, despite Plaintiff’s representations of good faith (ECF No. 3-1 at 9–10), the Court
22 shares the concern noted by other courts in this District of “unscrupulous tactics [being]
23 used by certain plaintiffs, especially in the adult film industry, to shake down the owners
24 of IP addresses’ to exact quick and quiet settlements from possibly innocent defendants
25 who pay out only to avoid potential embarrassment.” *Malibu Media, LLC v. Doe*, No. 16-
26 cv-00786-JLS-NLS, 2016 WL 9488778, at *4 (S.D. Cal. May 6, 2016) (quoting *Malibu*
27 *Media, LLC v. Does 1–5*, No. 12 Civ. 2950(JPO), 2012 WL 2001968, at *1 (S.D.N.Y. June
28 1, 2012)). The Court therefore finds that a limited protective order is necessary to protect

1 Defendant's privacy. Further, Plaintiff does not oppose a protective order establishing
2 procedural safeguards, "should the Court find such procedures to be appropriate." (ECF
3 No. 3-1 at 18.) Accordingly, the Court GRANTS Plaintiff's *ex parte* motion (ECF No. 4)
4 and **ORDERS** as follows:

5 1. Plaintiff may serve on AT&T U-verse a subpoena, pursuant to and compliant
6 with the procedures of Federal Rule of Civil Procedure 45, seeking only the name and
7 address of the subscriber assigned IP address 23.119.229.181 for the relevant time period
8 of the alleged infringement. Plaintiff shall not seek from AT&T U-verse any other
9 personally identifiable information about the subscriber.

10 2. Plaintiff's subpoena to AT&T U-verse must provide a minimum of forty-five
11 (45) calendar days' notice before any production responsive to the subpoena shall be made
12 to Plaintiff.

13 3. At the time Plaintiff serves its subpoena on AT&T U-verse, Plaintiff shall also
14 serve on AT&T U-verse a copy of this Order.

15 4. Within fourteen (14) calendar days after service of the subpoena, AT&T U-
16 verse shall notify the subscriber assigned IP address 23.119.229.181 that his, her, or its
17 identity has been subpoenaed by Plaintiff and shall provide the subscriber a copy of this
18 Order with the required notice.

19 5. The subscriber whose identity has been subpoenaed shall have thirty (30)
20 calendar days from the date of such notice to challenge AT&T U-verse's disclosure of his,
21 her, or its name and address by filing an appropriate pleading with this Court contesting
22 the subpoena.

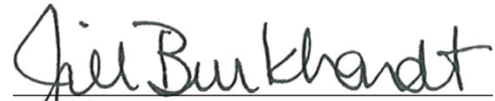
23 6. If AT&T U-verse seeks to modify or quash the subpoena, it shall do so as
24 provided by Federal Rule of Civil Procedure 45(d)(3).

25 7. In the event a motion to quash, modify, or otherwise challenge the subpoena
26 is brought properly before the Court, AT&T U-verse shall preserve the information sought
27 by the subpoena pending the resolution of any such motion.
28

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

6 **IT IS SO ORDERED.**

7 Dated: October 27, 2022

8 
9 Hon. Jill L. Burkhardt
10 United States Magistrate Judge

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