

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 70.95.155.251,
16 Defendant.

Case No.: 23-cv-01787-RBM-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.¹ Plaintiff
26

27
28 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*, *MILFY*, *Tushy*, *Tushy Raw*, *Vixen*, *Blacked Raw*, and *Slayed*. (ECF No.
3 1 ¶¶ 2–3.) Plaintiff alleges that between March 3, 2022, and September 4, 2023,² the person
4 or entity assigned Internet Protocol (“IP”) address 70.95.155.251 illegally downloaded and
5 distributed twenty-five 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 70.95.155.251” on September 27, 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”), Spectrum. (*Id.* ¶¶ 5, 13.) In the instant
13 Motion, Plaintiff asserts that Spectrum is the owner of Defendant’s IP address, and thus,
14 “is the only party with the information necessary to identify Defendant by correlating the
15 IP address with John Doe’s identity.” (ECF No. 4-1 at 7.) Plaintiff therefore seeks leave
16 to serve a Rule 45 subpoena on Spectrum requesting the true name and address associated
17 with IP address 70.95.155.251. (*Id.* at 7–8.) Without Defendant’s identity, Plaintiff cannot
18 serve Defendant and prosecute this case. (*Id.* at 8.)

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 70.95.155.251 engaged in allegedly infringing activity between
March 3, 2022, and September 4, 2023. (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, LLC*
8 *v. Does 1–46*, No. C-11-02263, 2011 WL 2470986, at *3 (N.D. Cal. June 21, 2011) (finding
9 that the plaintiff met its burden to identify the Doe defendants with sufficient specificity
10 by identifying the Doe defendants’ IP addresses and then using geolocation technology to
11 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 70.95.155.251 engaged in allegedly
15 infringing activity between March 3, 2022, and September 4, 2023, in San Diego,
16 California. (ECF No. 1-2.) To substantiate these claims, Plaintiff attached four
17 declarations to the 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. 4-2 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.* ¶¶ 52–56.) 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.* ¶¶ 43–51, 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. 4-2 at 16–22 (“Ex. B”).) Mr. Paige explains that VXN Scan “recorded numerous
18 BitTorrent computer transactions between the system and IP address 70.95.155.251 in the
19 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 September 4, 2023, “IP address 70.95.155.251 uploaded a piece or pieces of a file
22 corresponding to hash value E683F0F9D186007A2269919B201A6997AE284B76 to
23 VXN Scan.” (*Id.* ¶¶ 16–19.) The hash value, or Info Hash, is the data used by BitTorrent
24 to identify and locate other pieces of a desired file; in this case, the desired file contained
25 an infringing copy of one of Plaintiff’s movies. (*Id.* ¶ 22; *see also* ECF No. 1-2 at 1.)
26 Based on his experience in similar cases, Mr. Paige opines that Spectrum, Defendant’s ISP,
27 “is the only entity that can correlate the IP address [70.95.155.251] to its subscriber and
28

1 identify Defendant as the person assigned [this] IP address . . . during the time of the alleged
2 infringement.” (Ex. B ¶ 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 70.95.155.251 was identical, strikingly similar, or substantially similar to
6 one of Plaintiff’s original copyrighted works. (ECF No. 4-2 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. 4-2 at 27–30 (“Ex. D”).) Ms. Kennedy explains that after
11 Plaintiff received data from VXN Scan identifying IP address 70.95.155.251 as infringing
12 its movies, “the IP address was automatically inputted into Maxmind’s Geolocation
13 Database” on March 3, 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 70.95.155.251 again into the Maxmind Database “[p]rior to filing its Complaint” and
17 “before filing [her] [D]eclaration,” and both times the IP address “continued to trace to this
18

19
20 ³ 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 District.” (*Id.* ¶¶ 6–7.) In its Motion, Plaintiff argues that this Court has previously
2 “accepted Maxmind’s findings for purposes of allowing expedited discovery.” (ECF No.
3 4-1 at 13 (citing *Strike 3 Holdings, LLC v. Doe*, No. CV 17-2317-JAH (BLM), 2017 WL
4 6389848, at *2 (S.D. Cal. Dec. 14, 2017)).)

5 Based on Plaintiff’s IP address tracing efforts, the timing of its efforts, and Plaintiff’s
6 continued tracing of IP address 70.95.155.251 to a location within San Diego, California,
7 the Court concludes that Plaintiff has met its evidentiary burden of identifying Defendant
8 with sufficient specificity and has shown that Defendant’s IP address likely relates to a
9 physical address within the Court’s jurisdiction.

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

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

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

24 Further, as discussed above, Plaintiff retained Mr. Paige, a computer forensics
25 expert, who analyzed the data captured by VXN Scan and was able to determine that IP
26 address 70.95.155.251 was engaged in the allegedly infringing activity on
27 September 4, 2023. (*See Ex. B* ¶¶ 13–26.) Mr. Paige also opined that Defendant’s ISP is
28 the only entity that can correlate IP address 70.95.155.251 to its subscriber and identify

1 Defendant as the person assigned this IP address during the time of the alleged
2 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 Spectrum to IP address
6 70.95.155.251. 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 70.95.155.251 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 Spectrum, Defendant’s ISP, requesting “only
15 the true name and address” of Defendant, the subscriber of IP address 70.95.155.251.
16 (ECF No. 4-1 at 7–8.) Further, Plaintiff provides that Spectrum is the only entity that can
17 identify Defendant by his, her, or its IP address. (Ex. B ¶ 28.) Accordingly, the Court
18 finds that Plaintiff need not file the proposed subpoena with the Court.

19 **IV. CONCLUSION**

20 For the reasons set forth above, the Court finds good cause to grant Plaintiff leave to
21 serve a Rule 45 subpoena upon Spectrum in advance of the Rule 26(f) conference.
22 However, despite Plaintiff’s representations of good faith (ECF No. 4-1 at 9–10), the Court
23 shares the concern noted by other courts in this District of “unscrupulous tactics [being]
24 used by certain plaintiffs, especially in the adult film industry, to shake down the owners
25 of IP addresses’ to exact quick and quiet settlements from possibly innocent defendants
26 who pay out only to avoid potential embarrassment.” *Malibu Media, LLC v. Doe*, No. 16-
27 cv-00786-JLS-NLS, 2016 WL 9488778, at *4 (S.D. Cal. May 6, 2016) (quoting *Malibu*
28 *Media, LLC v. Does 1–5*, No. 12 Civ. 2950(JPO), 2012 WL 2001968, at *1 (S.D.N.Y. June

1 1, 2012)). The Court therefore finds that a limited protective order is necessary to protect
2 Defendant's privacy. Further, Plaintiff has invited the Court to issue a protective order
3 establishing procedural safeguards, "should the Court find such procedures to be
4 appropriate." (ECF No. 4-1 at 18.) Accordingly, the Court **GRANTS** Plaintiff's *ex parte*
5 Motion (ECF No. 4) and **ORDERS** as follows:

6 1. Plaintiff may serve on Spectrum a subpoena, pursuant to and compliant with
7 the procedures of Federal Rule of Civil Procedure 45, seeking only the name and address
8 of the subscriber assigned IP address 70.95.155.251 for the relevant time period of the
9 alleged infringement. Plaintiff shall not seek from Spectrum any other personally
10 identifiable information about the subscriber.

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

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

16 4. Within fourteen (14) calendar days after service of the subpoena, Spectrum
17 shall notify the subscriber assigned IP address 70.95.155.251 that his, her, or its identity
18 has been subpoenaed by Plaintiff and shall provide the subscriber a copy of this Order with
19 the required notice.

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

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

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

