

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 104.176.77.225,

Defendant.

Case No.: 3:23-cv-01788-GPC-AHG

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

[ECF No. 4]

Before the Court is Plaintiff Strike 3 Holdings, LLC’s (“Plaintiff”) *Ex-Parte* Application for Leave to Serve a Third-Party Subpoena Prior to a Rule 26(f) Conference. ECF No. 4. No defendant has been named or served, and so no opposition or reply briefs have been filed. For the reasons discussed below, the Court **GRANTS** Plaintiff’s *ex parte* application.

I. BACKGROUND

On September 27, 2023, Plaintiff filed a Complaint against Defendant “John Doe,” who is a subscriber of the Internet Service Provider (“ISP”) AT&T Internet, with assigned Internet Protocol (“IP”) address 104.176.77.225. ECF No. 1 ¶ 5. Plaintiff Strike 3 Holdings, LLC, is the owner of numerous adult motion pictures, which Plaintiff distributes through

1 adult websites and DVDs. *Id.* ¶¶ 2–3. Plaintiff asserts that Defendant is committing
2 “rampant and wholesale copyright infringement” by downloading, recording, and
3 distributing copies of Plaintiff’s copyrighted motion pictures without authorization through
4 the use of the BitTorrent file distribution network. *Id.* at ¶¶ 4, 18–44.

5 In the instant motion, Plaintiff seeks leave to conduct early discovery prior to the
6 mandated Rule 26(f) conference to learn Defendant’s identity. ECF No. 4. Specifically,
7 Plaintiff seeks an order permitting it to serve a third-party subpoena under Federal Rule of
8 Civil Procedure 45 on Defendant’s ISP, AT&T Internet (“AT&T”), which would require
9 AT&T to supply the name and address of Defendant John Doe to Plaintiff, so that Plaintiff
10 “may learn Defendant’s identity, further investigate Defendant’s role in the infringement,
11 and effectuate service.” ECF No. 4-1 at 7–8. Through service of the third-party subpoena,
12 Plaintiff seeks only “the true name and address of Defendant.” *Id.* at 8. Additionally,
13 Plaintiff represents to the Court that it will only use this information to prosecute the claims
14 made in its Complaint. *Id.*

15 II. LEGAL STANDARD

16 A party is generally not permitted to obtain discovery without a court order before
17 the parties have conferred pursuant to Federal Rule of Civil Procedure 26(f). Fed. R. Civ.
18 P. 26(d)(1). However, courts make exceptions to allow limited discovery after a complaint
19 is filed to permit the plaintiff to learn the identifying information necessary to serve the
20 defendant. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 577 (N.D. Cal. 1999);
21 *see, e.g., UMG Recordings, Inc. v. Doe*, No. C-08-3999-RMW, 2008 WL 4104207, at *2
22 (N.D. Cal. Aug. 29, 2008) (noting, in an infringement case, that “a plaintiff cannot have a
23 discovery planning conference with an anonymous defendant[,]” and limited expedited
24 discovery would thus “permit the [plaintiff] to identify John Doe and serve the defendant,
25 permitting this case to go forward.”).

26 Consistent with this generally recognized exception to Rule 26(f), the Ninth Circuit
27 has held that ““where the identity of the alleged defendant[] [is] not [] known prior to the
28 filing of a complaint[,] the plaintiff should be given an opportunity through discovery to

1 identify the unknown defendants, unless it is clear that discovery would not uncover the
2 identities, or that the complaint would be dismissed on other grounds.” *Wakefield v.*
3 *Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999) (quoting *Gillespie v. Civiletti*, 629 F.2d
4 637, 642 (9th Cir. 1980)).

5 A party who requests early or expedited discovery must make a showing of good
6 cause. *See Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 275–76 (N.D. Cal.
7 2002) (applying “the conventional standard of good cause in evaluating Plaintiff’s request
8 for expedited discovery”). Good cause is established through a balancing test “where the
9 need for expedited discovery, in consideration of the administration of justice, outweighs
10 the prejudice to the responding party.” *Id.* at 276. To determine whether “good cause”
11 exists to permit expedited discovery to identify John Doe defendants, district courts in the
12 Ninth Circuit consider whether the plaintiff (1) “identif[ies] the missing party with
13 sufficient specificity such that the Court can determine that the defendant is a real person
14 or entity who could be sued in federal court”; (2) “identif[ies] all previous steps taken to
15 locate the elusive defendant” to ensure that plaintiff has made a good faith effort to identify
16 the defendant; and (3) “establish[es] to the Court’s satisfaction that plaintiff’s suit against
17 defendant could withstand a motion to dismiss.” *Columbia Ins.*, 185 F.R.D. at 578–80.
18 Additionally, the plaintiff should demonstrate the discovery will likely lead to identifying
19 information that will permit service of process. *Id.* at 580. These factors are considered to
20 ensure the expedited discovery procedure “will only be employed in cases where the
21 plaintiff has in good faith exhausted traditional avenues for identifying a civil defendant
22 pre-service, and will prevent use of this method to harass or intimidate.” *Id.*

23 III. DISCUSSION

24 Plaintiff contends that there is good cause for this Court to allow expedited
25 discovery. ECF No. 4-1 at 11–18. For the reasons stated below, the Court agrees.

26 a. Identification of Missing Party with Sufficient Specificity

27 To satisfy the first prong, Plaintiff must identify Defendant with enough specificity
28 to enable the Court to determine that Defendant is a real person or entity who would be

1 subject to the jurisdiction of this Court. *Columbia Ins.*, 185 F.R.D. at 578. District courts
2 in this circuit have determined “a plaintiff identifies Doe defendants with sufficient
3 specificity by providing the unique IP addresses assigned to an individual defendant on the
4 day of the allegedly infringing conduct, and by using ‘geolocation technology’ to trace the
5 IP addresses to a physical point of origin.” *808 Holdings, LLC v. Collective of December*
6 *29, 2011 Sharing Hash*, No. 12cv186 MMA-RBB, 2012 WL 12884688, at *4 (S.D. Cal.
7 May 4, 2012); *see Openmind Solutions, Inc. v. Does 1-39*, No. C-11-3311-MEJ, 2011 WL
8 4715200, at *2 (N.D. Cal. Oct. 7, 2011) (concluding that plaintiff satisfied the first factor
9 by identifying the defendants’ IP addresses and by tracing the IP addresses to a point of
10 origin within the State of California); *Pink Lotus Entm’t, LLC v. Does 1-46*, No. C-11-
11 02263, 2011 WL 2470986, at *3 (N.D. Cal. June 21, 2011) (same). Other courts have
12 concluded that merely identifying the IP addresses on the day of the alleged infringement
13 satisfies this factor. *808 Holdings*, 2012 WL 12884688, at *4 (collecting cases).

14 Here, Plaintiff has identified the Doe Defendant with sufficient specificity. First, in
15 support of the present motion, Plaintiff provided an 81-paragraph Declaration of David
16 Williamson, an independent contractor hired by Plaintiff as an Information Systems and
17 Management Consultant. ECF No. 4-2 at 2–15 (“Ex. A”). In that role, Mr. Williamson
18 testifies he “oversaw the design, development, and overall creation of the infringement
19 detection system called VXN Scan[,] which [Plaintiff] both owns and uses to identify the
20 IP addresses used by individuals infringing Plaintiff’s movies via the BitTorrent protocol.”
21 Ex. A, ¶ 40. Mr. Williamson’s Declaration explains the VXN Scan system in detail, which
22 involves, in part, the development of a proprietary BitTorrent client that emulates the
23 behavior of a standard BitTorrent client by repeatedly downloading data pieces from peers
24 within the BitTorrent network that are distributing Plaintiff’s movies. *Id.* ¶¶ 52–55.
25 Mr. Williamson testifies that another component of the VXN Scan system is the PCAP¹
26

27
28 ¹ PCAP stands for “Packet Capture.” Ex. A at ¶ 58.

1 Recorder / Capture Card, which is able to record the IP addresses connecting to the
2 Proprietary Client and sending the infringed copies of Plaintiff’s movies to the Proprietary
3 Client through the BitTorrent network. *Id.* ¶¶ 57–59. Not only does a PCAP contain the IP
4 addresses used in the network transaction, it also records the port number and BitTorrent
5 client used to accomplish each transaction, and the “Info Hash” associated with the
6 infringing computer file, which reflects the metadata of the particular underlying .torrent
7 file being shared without authorization. *Id.* ¶¶ 61–62. VXN uses a PCAP Capture Card
8 called Link™ NT40A01 SmartNIC, which records PCAPs in real time, and is able to record
9 perfect copies of every network packet received by the Proprietary Client via a passive
10 network tap. *Id.* ¶¶ 63–65. Although this Order touches only on two of the components of
11 the VXN Scan system, Mr. Williamson’s 81-paragraph Declaration sets forth additional
12 in-depth details of all five components of the system, providing the Court a thorough
13 understanding of how the system reliably pinpoints the IP addresses used by individuals
14 infringing Plaintiff’s movies and verifies the infringement.

15 Second, Plaintiff also provided a declaration by Patrick Paige, a computer forensics
16 expert retained by Plaintiff to analyze and retain forensic evidence captured by the VXN
17 Scan system. ECF No. 4-2 at 17–22 (“Ex. B”). Mr. Paige explains that VXN Scan recorded
18 numerous BitTorrent computer transactions with IP address 104.176.77.225 in the form of
19 PCAPs, and that he reviewed the PCAP to confirm that it evidences a recorded transaction
20 with that IP address on August 25, 2023 at 18:51:30 UTC involving the IP address
21 uploading a piece or pieces of a file corresponding to the hash value that is unique to one
22 of Plaintiff’s movies. Ex. B, ¶¶ 13–26.

23 Third, Plaintiff provided a declaration by Susan Stalzer, one of Plaintiff’s employees
24 who verified that each digital media file obtained using the VXN Scan’s Torrent Collector
25 and Downloader components was a copy of one of Plaintiff’s copyrighted works, by
26 viewing the unauthorized motion pictures corresponding with the file hashes side-by-side
27 with Plaintiff’s original movies. ECF No. 4-2 at 7-11 (“Ex. C”); *see also* ECF No. 1-2
28

1 (Exhibit A to the Complaint, listing the hash values of the 24 torrent files received by the
2 Proprietary Client from the IP address 104.176.77.225).

3 Finally, Plaintiff explains that it used Maxmind, a geolocation technology, to trace
4 Defendant's IP address to a geographic area within this Court's personal jurisdiction. ECF
5 No. 4-1 at 12-13. To elaborate on this point, Plaintiff provides a declaration by Emilie
6 Kennedy, Plaintiff's in-house General Counsel. ECF No. 4-2 at 28–30 ("Ex. D"). Ms.
7 Kennedy explains that after Plaintiff received infringement data from VXXN Scan
8 identifying IP address 104.176.77.225 as infringing its works, the IP address was
9 automatically input into Maxmind's Geolocation Database on May 17, 2022 at 00:22:36
10 UTC, which traced the IP address location to San Diego, California, within this Court's
11 jurisdiction. Ex. D, ¶¶ 4–5. Plaintiff has since repeated the trace through the Maxmind
12 Geolocation Database twice more, prior to filing the Complaint and prior to filing the
13 present Motion, confirming the IP address continues to trace to San Diego and this District.
14 *Id.* ¶¶ 6–7. The Court is satisfied that these multiple geolocation traces over the course of
15 17 months indicating that the Defendant is located in this District are reliably accurate.

16 Based on all of the information above, the Court concludes that Plaintiff has
17 provided a sufficient showing that it seeks to sue a real person subject to the Court's
18 jurisdiction. Likewise, if Plaintiff obtains the identifying information from the ISP for the
19 subscriber assigned the IP address at issue, the information sought in the subpoena would
20 likely enable Plaintiff to serve Defendant. Therefore, the Court finds Plaintiff satisfied the
21 "sufficient specificity" threshold.

22 **b. Previous Attempts to Locate Defendant**

23 Next, Plaintiff is required to describe all steps taken to identify the Doe defendant in
24 a good-faith effort to locate and serve them. Plaintiff states that it attempted to locate
25 Defendant by searching for Defendant's IP address using online search engines and other
26 web search tools. ECF No. 4-1 at 14. Plaintiff also reviewed numerous sources of authority
27 such as legislative reports, agency websites, and informational technology guides,
28 regarding whether it is possible to identify such a defendant by other means, and

1 extensively discussed this issue with its computer investigators and cyber security
2 consultants. *Id.* Despite these diligent efforts, Plaintiff was unable to identify any means of
3 obtaining the identities of an accused infringer such as Defendant other than through
4 subpoenaing the information from Defendant’s ISP. *Id.* In his Declaration, Mr. Paige
5 testified that based on his experience in similar cases, Defendant’s ISP, AT&T Internet, is
6 the only entity that can correlate the IP address 104.176.77.225 to its subscriber to identify
7 Defendant. Ex. B ¶ 28. Thus, the Court finds Plaintiff has shown it has made a good-faith
8 effort to identify and locate Defendant through other means before resorting to filing the
9 instant motion.

10 **c. Whether Plaintiff Can Withstand a Motion to Dismiss**

11 Lastly, Plaintiff must establish it could survive a motion to dismiss. *See* Fed. R. Civ.
12 P. 12(b); *Columbia Ins.*, 185 F.R.D. at 579. To survive a motion to dismiss for failure to
13 state a claim upon which relief can be granted, “a complaint must contain sufficient factual
14 matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v.*
15 *Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570
16 (2007)). To present a prima facie case of copyright infringement, Plaintiff must show: (1)
17 ownership of a valid copyright; and (2) that Defendant violated the copyright owner’s
18 exclusive rights under the Copyright Act. *Range Road Music, Inc. v. East Coast Foods,*
19 *Inc.*, 668 F.3d 1148, 1153 (9th Cir. 2012). In addition, for direct infringement Plaintiff is
20 required to show causation by Defendant. *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657,
21 666 (9th Cir. 2017).

22 Here, Plaintiff’s Complaint clearly alleges that Plaintiff owns a valid copyright in
23 the works at issue, which are registered with the United States Copyright Office. *See* ECF
24 No. 1 ¶¶ 43, 46, 49.² And again, Ms. Stalzer attests that she reviewed the files correlating
25

26
27
28 ² Exhibit A to the Complaint, which shows the hash values of the purportedly infringing
movies downloaded from the IP address 104.176.77.225, also contains the United States

1 to the hashes identified in Exhibit A to the Complaint and confirmed that they are
2 “identical, strikingly similar or substantially similar” to Strike 3’s original copyrighted
3 Works. Ex. C ¶¶ 7–11; ECF No. 1 ¶¶ 34–35. Plaintiff’s Complaint also alleges Defendant
4 used BitTorrent to copy and distribute the copyrighted works without authorization, and
5 that the infringement was continuous and ongoing. ECF No. 1 ¶¶ 4, 19–30, 33, 33–36, 44–
6 46. Thus, Plaintiff’s Complaint has stated a claim for copyright infringement against the
7 Doe Defendant sufficient to survive a motion to dismiss. Additionally, Plaintiff has alleged
8 sufficient facts to show it could withstand a motion to dismiss for lack of personal
9 jurisdiction or a motion for improper venue, because Defendant’s IP address was traced to
10 a location in this District. Accordingly, the Court concludes Plaintiff has met the third
11 prong necessary to establish good cause for granting early discovery.

12 **IV. CONCLUSION**

13 For the reasons set forth above, and for good cause shown, the Court **GRANTS**
14 Plaintiff’s *ex parte* application for leave to serve a subpoena prior to a Rule 26(f)
15 conference. ECF No. 4. However, the Court is cognizant of the potential embarrassment of
16 being identified in this type of case and “shares the growing concern about unscrupulous
17 tactics used by certain plaintiffs, especially in the adult film industry, to shake down the
18 owners of IP addresses.” *Malibu Media, LLC v. Does 1-5*, No. 12-Civ-2950-JPO, 2012 WL
19 2001968, at *1 (S.D.N.Y. June 1, 2012). Anticipating and sharing these concerns, Plaintiff
20 invites the Court to issue a protective order establishing procedural safeguards if the Court
21 finds such procedures appropriate. ECF No. 4-1 at 18 (citing *Strike 3 Holdings, LLC v.*
22 *Doe*, No. 17CV2317-JAH (BLM), 2017 WL 6389848, at *3-*4 (S.D. Cal. Dec. 14, 2017)
23 and *Strike 3 Holdings, LLC v. Doe*, No. 1:18-CV-12585-NLH-JS, 2020 WL 3567282
24 (D.N.J. June 30, 2020)). Accordingly, the Court **ORDERS** as follows:

- 25 1. Plaintiff shall attach a copy of this Order to any subpoena.

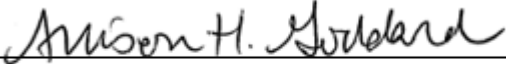
26
27
28 Copyright Office registration information of the works that correspond with those hash
files. ECF No. 1-2.

- 1 2. Plaintiff may serve the ISP, AT&T Internet, with a Rule 45 subpoena
2 commanding the ISP to provide Plaintiff with **only** the true name and address
3 of the Defendant to whom the ISP assigned an IP address as set forth on
4 Exhibit A to the Complaint. The ISP is **not** to release the Defendant’s
5 telephone number or email address.
- 6 3. Plaintiff may also serve a Rule 45 subpoena in the same manner as above on
7 any service provider that is identified in response to a subpoena as a provider
8 of Internet services to Defendant.
- 9 4. Within fourteen (14) calendar days after service of the subpoena, the ISP shall
10 notify the subscriber that his or her identity has been subpoenaed by Plaintiff,
11 in compliance with 47 U.S.C. § 551(c)(2)(B) (“A cable operator may disclose
12 such [personal identifying] information if the disclosure is . . . made pursuant
13 to a court order authorizing such disclosure, if the subscriber is notified of
14 such order by the person to whom the order is directed.”). The ISP must also
15 provide a copy of this Order along with the required notice to the subscriber
16 whose identity is sought pursuant to this Order.
- 17 5. The subscriber whose identity has been subpoenaed shall have thirty (30)
18 calendar days from the date of such notice to challenge the disclosure of his
19 or her name and contact information by filing an appropriate pleading with
20 this Court contesting the subpoena. A subscriber who moves to quash or
21 modify the subpoena may proceed anonymously as “John Doe,” and shall
22 remain anonymous until the Court orders that the identifying information may
23 be released.
- 24 6. If the ISP wishes to move to quash the subpoena, it shall do so before the
25 return date of the subpoena. The return date of the subpoena must allow for at
26 least forty-five (45) days from service to production. If a motion to quash or
27 other challenge is brought, the ISP shall preserve the information sought by
28 Plaintiff in the subpoena pending resolution of such motion or challenge.

1 7. Plaintiff may only use the information disclosed in response to a Rule 45
2 subpoena served on the ISP for the purpose of protecting and enforcing
3 Plaintiff's rights as set forth in its Complaint. If Defendant wishes to proceed
4 anonymously, Plaintiff may not release any identifying information without a
5 court order allowing the release of the information.

6 **IT IS SO ORDERED.**

7
8 Dated: October 19, 2023

9 
10

Honorable Allison H. Goddard
United States Magistrate Judge