

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
75.50.122.76,

Defendant.

Case No.: 23cv1381-RBM (MSB)

**ORDER GRANTING PLAINTIFF’S EX
PARTE APPLICATION FOR LEAVE TO
SERVE A THIRD-PARTY SUBPOENA
PRIOR TO A RULE 26(f) CONFERENCE
[ECF NO. 4]**

On August 10, 2023, Plaintiff Strike 3 Holdings, LLC (“Strike 3”) filed an “Ex-Parte Application for Leave to Serve a Third-Party Subpoena Prior to a Rule 26(f) Conference” (“Ex Parte Application”). (ECF No. 4.) Plaintiff seeks to subpoena Defendant John Doe’s Internet Service Provider (“ISP”) AT&T Internet for “limited, immediate discovery . . . so that Plaintiff may learn Defendant’s identity, further investigate Defendant’s role in the infringement, and effectuate service.” (ECF No. 4-1 at 7–8.) Because Defendant has not been identified, no opposition or reply briefs have been filed. For the following reasons, the Ex Parte Application is **GRANTED**.

///
///
///

1 **I. BACKGROUND**

2 Plaintiff owns the copyright to certain motion pictures. (ECF No. 4-1 at 7.) On July
3 28, 2023, Plaintiff filed a Complaint alleging that Defendant John Doe, an internet
4 subscriber assigned Internet Protocol (“IP”) address 75.50.122.76, has been using the
5 BitTorrent protocol to commit “rampant and wholesale copyright infringement” by
6 downloading and distributing twenty-four of Plaintiff’s copyrighted works over an
7 extended period. (ECF No. 1 at 1–2.) Plaintiff alleges it used its proprietary forensic
8 software, VXN Scan, to discover that Defendant’s IP address was illegally distributing
9 Plaintiff’s copyrighted motion pictures. (ECF No. 4-1 at 7; ECF No. 4-2 at 20–21.)

10 On August 10, 2023, Plaintiff filed the instant Ex Parte Application to seek leave to
11 serve a subpoena pursuant to Federal Rule of Civil Procedure 45 on Defendant’s ISP,
12 AT&T Internet. (ECF No. 4-1 at 7.) Plaintiff maintains that the Rule 45 subpoena “will
13 only demand the true name and address of Defendant[,]” and Plaintiff “will only use this
14 information to prosecute the claims made in its Complaint.” (Id. at 8.) Plaintiff further
15 claims that “[w]ithout this information, Plaintiff cannot serve Defendant nor pursue this
16 lawsuit and protect its copyrights.” (Id.)

17 **II. LEGAL STANDARD**

18 Generally, formal discovery is not permitted before the parties have conferred
19 pursuant to Federal Rule of Civil Procedure 26(f). Fed. R. Civ. P. 26(d)(1). Courts,
20 however, have made exceptions “in rare cases . . . permitting limited discovery to ensue
21 after filing of the complaint to permit the plaintiff to learn the identifying facts
22 necessary to permit service on the defendant.” Columbia Ins. Co. v. Seescandy.com, 185
23 F.R.D. 573, 577 (N.D. Cal. 1999). Courts in the Ninth Circuit apply a “good cause”
24 standard to decide whether to permit early discovery. Semitool, Inc. v. Tokyo Electron
25 Am., Inc., 208 F.R.D. 273, 275–76 (N.D. Cal. 2002). “Good cause” is established “where
26 the need for expedited discovery, in consideration of the administration of justice,
27 outweighs the prejudice to the responding party.” Id.

1 “[W]hen the defendants’ identities are unknown at the time the complaint is
2 filed, courts may grant plaintiffs leave to take early discovery to determine the
3 defendants’ identities ‘unless it is clear that discovery would not uncover the identities,
4 or that the complaint would be dismissed on other grounds.’” 808 Holdings, LLC v.
5 Collective of Dec. 29, 2011 Sharing Hash E37917C8EEB4585E6421358FF32F29C
6 D63C23C91, No. 12cv186-MMA (RBB), 2012 WL 12884688, at *3 (S.D. Cal. May 8, 2012)
7 (quoting Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir. 1980)). “A district court’s
8 decision to grant discovery to determine jurisdictional facts is a matter of discretion.”
9 Columbia Ins. Co., 185 F.R.D. at 578.

10 District Courts in the Ninth Circuit typically apply a three-factor test when
11 considering motions for early discovery to identify Doe defendants. Id. at 578–80. First,
12 the moving party should be able to “identify the missing party with sufficient specificity
13 [] that the Court can determine that [the] defendant is a real person or entity who could
14 be sued in federal court.” Id. at 578. Second, the movant “should identify all previous
15 steps taken to locate the elusive defendant” to ensure “that [the movant has made] a
16 good faith effort to comply with the requirements of the service of process and
17 specifically identifying defendants.” Id. at 579. Third, the plaintiff “should establish to
18 the Court’s satisfaction that plaintiff’s suit against defendant could withstand a motion
19 to dismiss.” Id.; see also Gillespie, 629 F.2d at 642 (stating early discovery to identify
20 unknown defendants should be permitted unless the complaint would be dismissed on
21 other grounds).

22 In addition to satisfying all three factors, plaintiff should provide “reasons
23 justifying the specific discovery requested [and] identification of a limited number of
24 persons or entities on whom discovery process might be served and for which there is a
25 reasonable likelihood that the discovery process will lead to identifying information
26 about defendant that would make service of process possible.” Columbia Ins. Co., 185
27 F.R.D. at 580; see also Gillespie, 629 F.2d at 642 (explaining that early discovery is
28 precluded if it is not likely to provide the identity of the defendant). These safeguards

1 are intended to ensure that early discovery “will only be employed in cases where the
2 plaintiff has in good faith exhausted traditional avenues for identifying a civil defendant
3 pre-service, and will prevent the use of this method to harass or intimidate.” Columbia
4 Ins. Co., 185 F.R.D. at 578.

5 III. ANALYSIS

6 Plaintiff seeks leave to serve a subpoena pursuant to Federal Rule of Civil
7 Procedure 45 on Defendant’s ISP, AT&T Internet. (ECF No. 4-1 at 7.) The Cable Privacy
8 Act generally prohibits a cable operator from disclosing “personally identifiable
9 information concerning any subscriber without the prior written or electronic consent of
10 the subscriber concerned.” 47 U.S.C. § 551(c)(1). A cable operator, however, may
11 disclose the information if the disclosure is made pursuant to a court order and the
12 cable operator notifies the subscriber of the order. 47 U.S.C. § 551(c)(2)(B). A cable
13 operator is “any person or group of persons” who “provides cable service over a cable
14 system and directly or through one or more affiliates owns a significant interest in such
15 cable system,” or “otherwise controls or is responsible for, through any arrangement,
16 the management and operation of such a cable system.” 47 U.S.C. § 522(5).

17 AT&T Internet is a cable operator, and the information Plaintiff seeks falls within
18 the exception to the Cable Privacy Act’s disclosure prohibition. See 47 U.S.C.
19 §551(c)(2)(B). Accordingly, if Plaintiff satisfies the multi-factor test used by district
20 courts to determine whether early discovery is warranted, Defendant’s ISP may disclose
21 the requested information pursuant to this Court’s order.

22 A. Plaintiff Has Identified Defendant with Sufficient Specificity

23 Plaintiff must identify Defendant with enough specificity to allow the Court to
24 determine that Defendant is a real person or entity, subject to the jurisdiction of this
25 Court. See Columbia Ins. Co., 185 F.R.D. at 578. “[A] plaintiff identifies Doe defendants
26 with sufficient specificity by providing the unique IP addresses assigned to an individual
27 defendant on the day of the allegedly infringing conduct, and by using ‘geolocation
28

1 technology' to trace the IP addresses to a physical point of origin." 808 Holdings, LLC,
2 2012 WL 12884688, at *4.

3 In support of its Ex Parte Application, Plaintiff submitted the Declaration of David
4 Williamson, an Information Systems and Management Consultant. (See ECF No. 4-2 at
5 3.) Mr. Williamson uses Plaintiff's infringement detection system, VXN Scan, to identify
6 the IP addresses used by individuals infringing Plaintiff's movies through the BitTorrent
7 protocol. (Id. at 8.) Further, although the BitTorrent protocol contains some default
8 and automatic functions, the functions that Plaintiff accuses Defendant of using require
9 human operation. See Christopher Civil, Mass Copyright Infringement Litigation: Of
10 Trolls, Pornography, Settlement and Joinder, 30 Syracuse J. Sci. & Tech. L. 2, 12 (2014)
11 ("BitTorrent transfers do not involve a centralized server that hosts or transfers the data
12 files in question. Instead, BitTorrent involves users interacting directly with other users
13 to upload and download the content."). Accordingly, Plaintiff has established that an
14 actual human was involved in the downloading and sharing of Plaintiff's allegedly
15 infringed works.

16 Plaintiff also submitted the Declaration of Patrick Paige, a Managing Member at
17 Computer Forensics, LLC, where Mr. Paige contends that he utilized Packet Capture
18 ("PCAP"), "a computer file containing captured or recorded data transmitted between
19 network devices[,] and VXN Scan to connect Defendant's IP address to the alleged
20 "piece of an infringing copy of Plaintiff's works." (ECF No. 4-2 at 18, 20.) According to
21 Mr. Paige, "[t]he PCAP contains a record data concerning that transaction, including, but
22 not limited to, the [IP] Addresses used in the network transaction, the date and time of
23 the network transaction, the port number used to accomplish each network transaction,
24 and the Info Hash value that the VXN Scan used as the subject of its request for data."
25 (Id. at 20.) Mr. Paige contends that the contents of the PCAP confirm that the infringing
26 activity connected to the IP address 75.50.122.76 was initiated on June 24, 2023, at
27 02:13:56 UTC. (Id.) Mr. Paige concludes that "the PCAP evidence shows that within that
28 transaction, IP address 75.50.122.76 uploaded a piece or pieces of a file corresponding

1 to hash value [representing Plaintiff's works] to VXN Scan." (Id.) This date and time
2 correspond with the date and time when one of Plaintiff's works were allegedly illegally
3 downloaded according to Exhibit A of Plaintiff's Complaint.¹ (ECF No. 5-1 at 10.)

4 In addition, Plaintiff submitted the Declaration of Emilie Kennedy, Plaintiff's in-
5 house General Counsel, in which Ms. Kennedy asserts geolocation was done by an
6 unspecified person to identify the location of Defendant on three separate occasions.
7 (ECF No. 4-2 at 29.) First, "[a]fter [Plaintiff] received infringement data from VXN Scan
8 identifying IP address 75.50.122.76 as infringing its works, the IP address was
9 automatically inputted into Maxmind's Geolocation Database." (Id.) Based on this
10 search, Ms. Kennedy contends that "Maxmind determined that the IP address traced to
11 a location in San Diego, California, which is within this Court's jurisdiction." (Id.)
12 Defendant's IP address was subsequently inputted by Plaintiff into Maxmind's Database
13 prior to the filing of Plaintiff's Complaint, and prior to the filing of her Declaration. (Id.)
14 On both occasions the IP address linked to Defendant, 75.50.122.76, traced to this
15 District.²

16 Plaintiff has provided sufficient information about infringing activity tied to
17 Defendant's unique IP address, the specific date and time associated with the activity,
18 and the location of the activity. Therefore, Plaintiff has demonstrated with sufficient
19 specificity that Defendant is a real person or entity, likely subject to the jurisdiction of
20 this Court. See Crim. Prods., Inc. v. Doe-72.192.163.220, Case No. 16cv2589-WQH (JLB),
21 2016 WL 6822186, at *3 (S.D. Cal. Nov. 18, 2016) (holding that the sufficient specificity
22 threshold is satisfied when the IP address identified by Maxmind geolocation services
23 identifies a physical location within the court's jurisdiction).

24 ///

25
26 ¹ Plaintiff filed a Notice of Errata attaching Exhibit A because it was missing from the original
Complaint. (ECF No. 5.)

27 ² Attached as Exhibit 1 to Ms. Kennedy's Declaration is a chart reflecting the results of the third and
28 final MaxMind Database search, showing the IP address alleged to be involved in the illegal downloads
and confirming that the location traces to San Diego, CA. (ECF No. 4-2 at 32.)

1 **B. Plaintiff Made a Good Faith Effort to Identify Defendant**

2 Plaintiff must also demonstrate that it has taken previous steps to locate and
3 serve the Defendant. See Columbia Ins. Co., 185 F.R.D. at 579. Although Plaintiff
4 maintains it diligently attempted to identify Defendant by searching for Defendant’s IP
5 address “on various web search tools, including basic search engines like
6 www.google.com,” Plaintiff does not submit evidence supporting this claim. (ECF No. 4-
7 1 at 14.) However, Ms. Kennedy’s Declaration and the MaxMind results attached as
8 Exhibit 1 indicate that Plaintiff took substantial steps to locate Defendant’s IP address
9 and identify Defendant’s ISP. (ECF No. 4-2 at 29–32.) Despite these efforts, Plaintiff was
10 unable to correlate the IP address to Defendant’s identity. Plaintiff maintains that it has
11 been “unable to identify any other way to go about obtaining the identities of its
12 infringers and does not know how else it could possibly enforce its copyrights from
13 illegal piracy over the Internet.” (ECF No. 4-1 at 14.) The Court therefore finds that
14 Plaintiff has made a good faith effort to identify, locate, and serve the Defendant. See
15 Malibu Media, LLC v. John Does 1 through 6, No. 12cv1355-LAB (DHB), 2012 WL
16 4471538, at *3 (S.D. Cal. Sept. 26, 2012) (finding plaintiff’s efforts to identify Doe
17 defendant were sufficient because “there is no other way for [p]laintiff to obtain
18 [d]efendants’ identities, except by serving a subpoena on [d]efendants’ ISPs demanding
19 it[.]”); see also Digital Sin, Inc. v. Does 1-5698, No. C 11-04397 LB, 2011 WL 5362068, at
20 *2 (N.D. Cal. Nov. 4, 2011) (finding plaintiff’s attempts to identify and locate defendant
21 sufficient, where the plaintiff “investigated and collected data on unauthorized
22 distribution of copies of the [alleged infringed work] on BitTorrent-based peer-to-peer
23 networks.”).

24 **C. Plaintiff’s Suit Could Withstand a Motion to Dismiss**

25 Plaintiff must further show that the Complaint in this case could withstand a
26 motion to dismiss. See Columbia Ins. Co., 185 F.R.D. at 579. A suit may be dismissed
27 pursuant to Rule 12(b) on several bases. Of all the bases that bear dismissal, those
28 relevant here are lack of subject matter jurisdiction, lack of personal jurisdiction, and

1 failure to state a claim. Fed. R. Civ. P. 12(b)(1), (2), (6). As to both subject matter and
2 personal jurisdiction, Plaintiff has alleged facts sufficient to survive a motion to dismiss.
3 For subject matter jurisdiction, Plaintiff’s Complaint alleges that “[t]his Court has subject
4 matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 (federal question); and
5 28 U.S.C. § 1338 (jurisdiction over copyright actions).” (ECF No. 1 at 2.) On the issue of
6 personal jurisdiction, Plaintiff maintains it used geolocation technology to determine
7 that Defendant’s IP address correlates to a physical address in the Southern District of
8 California. (Id. at 2–3.)

9 A motion to dismiss under Rule 12(b)(6) of the Federal Rules of Civil Procedure
10 tests the sufficiency of the allegations in the Complaint. Navarro v. Block, 250 F.3d 729,
11 732 (9th Cir. 2001). Plaintiff’s Complaint alleges a single cause of action against
12 Defendant for direct copyright infringement. (ECF No. 1 at 7–9.) To allege a claim for
13 direct copyright infringement, a plaintiff must show: “(1) ownership of a valid copyright;
14 and (2) that the defendant violated the copyright owner’s exclusive rights under the
15 Copyright Act.” Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004). “In addition,
16 direct infringement requires the plaintiff to show causation (also referred to as
17 ‘volitional conduct’) by the defendant.” Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657,
18 666 (9th Cir. 2017).

19 Plaintiff alleges it owns the copyrights to the works that are the subject of this suit
20 and claims that the works “have been registered with the United States Copyright
21 Office.” (ECF No. 1 at 7.) Plaintiff also alleges that Defendant “used the BitTorrent file
22 network to illegally download and distribute Plaintiff’s copyrighted motion pictures[,]”
23 and did so “without authorization.” (Id. at 5, 7.) Assuming Plaintiff’s allegations are
24 true, they state a claim on which relief can be granted. See A&M Recs., Inc. v. Napster,
25 Inc., 239 F.3d 1004, 1013–14 (9th Cir. 2001) (finding plaintiffs sufficiently demonstrated
26 ownership and infringement by showing Napster allowed its users to download
27 copyrighted music, up to seventy percent of which was owned or administered by the
28 plaintiffs); see also Malibu Media, LLC v. Doe, Case No. 16cv1916-GPC (JMA), 2016 WL

1 6216183, at *2 (S.D. Cal. Oct. 25, 2016) (holding that plaintiff alleged a prima facie case
2 of copyright infringement against defendant by alleging that plaintiff owned twelve
3 copyrighted movies at issue, and that defendant infringed plaintiff's copyrights by
4 copying and distributing plaintiff's movies through the BitTorrent network without
5 plaintiff's permission). Therefore, Plaintiff has sufficiently alleged the prima facie
6 elements of copyright infringement, and the Complaint will likely withstand a motion to
7 dismiss.

8 **D. Whether Requested Discovery Will Lead to Identifying Information**

9 Finally, Plaintiff is required to demonstrate that "there is a reasonable likelihood
10 that the discovery process will lead to identifying information about defendant that
11 would make service of process possible." Columbia Ins. Co., 185 F.R.D. at 580. As
12 discussed above, Plaintiff's forensic investigation uncovered the unique IP address
13 75.50.122.76. (ECF No. 4-2 at 20.) Further, Exhibit 1 to Emilie Kennedy's declaration
14 indicates that her MaxMind search revealed that the ISP AT&T Internet owned
15 Defendant's IP address at the time of the infringement. (Id. at 32.) Based on his
16 experience in similar cases, Mr. Paige explains that "AT&T Internet is the only entity that
17 can correlate" Defendant's IP address to the IP address owner's identity. (Id. at 22.)
18 Accordingly, if AT&T Internet provides Plaintiff with Defendant's name and address, this
19 will likely lead to information making it possible for Plaintiff to effectuate service on
20 Defendant.

21 **IV. CONCLUSION**

22 For the foregoing reasons, the Court **GRANTS** the Ex Parte Application for Leave
23 to Serve a Third-Party Subpoena Prior to a Rule 26(f) Conference [ECF No. 4] as follows:

24 1. Plaintiff may serve a subpoena pursuant to Federal Rule of Civil Procedure
25 45 on AT&T Internet, seeking only the name and address of the subscriber assigned to
26 the IP address 75.50.122.76. Plaintiff may not subpoena additional information about
27 the subscriber;

28 ///

1 2. Plaintiff may only use the disclosed information to protect its copyrights in
2 the instant litigation;

3 3. Within fourteen (14) calendar days after service of the subpoena, AT&T
4 Internet shall notify the subscriber assigned the IP address 75.50.122.76 that his, her, or
5 its identity has been subpoenaed by Plaintiff;

6 4. The subscriber whose identity has been subpoenaed shall have thirty (30)
7 calendar days from the date of the notice to challenge the disclosure of his, her, or its
8 name and address by filing an appropriate pleading with this Court contesting the
9 subpoena;

10 5. If AT&T Internet wishes to move to quash the subpoena, it shall do so
11 before the return date of the subpoena. The return date of the subpoena must allow
12 for at least forty-five (45) days from service to production. If a motion to quash or other
13 customer challenge is brought, AT&T Internet shall preserve the information sought by
14 Plaintiff in the subpoena pending resolution of the motion or challenge;

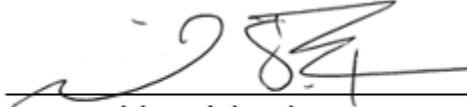
15 6. Plaintiff shall serve a copy of this Order with any subpoena obtained and
16 served to AT&T Internet pursuant to this Order;

17 7. AT&T Internet must provide a copy of this Order along with the required
18 notice to the subscriber whose identity is sought pursuant to this Order.

19 8. No other discovery is authorized at this time.

20 **IT IS SO ORDERED.**

21 Dated: August 18, 2023

22 
23 _____
24 Honorable Michael S. Berg
25 United States Magistrate Judge
26
27
28