

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

Background

Plaintiff filed a Complaint against defendant alleging a single cause of action for direct copyright infringement. [Doc. No. 1, at pp. 6-8]. In the Complaint, plaintiff asserts ownership of copyrights for adult motion pictures that are distributed through adult websites and DVDs. [Doc. No. 1, at pp. 1-2, 6.] The Complaint alleges that the defendant is using BitTorrent protocol to download and distribute plaintiff's motion pictures to others "on a grand scale." [Doc. No. 1, at p. 2.] The Complaint further alleges that defendant "downloaded, copied, and distributed a complete copy" of plaintiff's copyrighted movies "without authorization." [Doc. No. 1, at p. 6.] According to the Complaint, defendant's "infringement is continuous and ongoing" and the lawsuit is the only way to effectively prevent defendant from infringing the copyrights. [Doc. No. 1, at p. 6.]

The Complaint explains that "BitTorrent is a system designed to quickly distribute large files over the Internet. Instead of downloading a file, such as a movie, from a single source, BitTorrent users are able to connect to the computers of other BitTorrent users in order to simultaneously download and upload pieces of the film from and to other users." [Doc. No. 1, at p. 4.] "To use BitTorrent to download a movie, the user has to obtain a 'torrent' file for that movie, from a torrent website. The torrent file contains instructions for identifying the Internet addresses of other BitTorrent users who have the movie, and for downloading the movie from those users. Once a user downloads all of the pieces of that movie from the other BitTorrent users, the movie is automatically reassembled into its original form, ready for playing." [Doc. No. 1, at p. 4.]

23
24
25
26
27
28

Discussion

In the *Ex Parte* Application, plaintiff seeks leave to serve limited, immediate discovery on defendant's Internet Service Provider ("ISP"), AT&T Inc. and/or AT&T U-verse, so that plaintiff may learn defendant's identity. [Doc. No. 4-1, at pp. 6-7]. Specifically, plaintiff seeks an order permitting it to serve a Rule 45 subpoena on AT&T Inc. (AT&T U-verse) to obtain the name and address of the account holder assigned to Internet Protocol ("IP") address 99.26.127.96. [Doc. No. 4-1, at pp. 6-7.]

1 Generally, discovery is not permitted without a court order before the parties have
2 conferred pursuant to Federal Rule of Civil Procedure 26(f). Fed. R. Civ. P. 26(d)(1). In
3 the Ninth Circuit, exceptions to requests for early discovery have generally been
4 disfavored. *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980). However, “situations
5 arise, such as the present, where the identity of alleged defendants will not be known prior
6 to the filing of a complaint. In such circumstances, the plaintiff should be given an
7 opportunity through discovery to identify the unknown defendants, unless it is clear that
8 discovery would not uncover the identities, or that the complaint would be dismissed on
9 other grounds.” *Id.*

10 “[S]ome limiting principals should apply to the determination of whether discovery
11 to uncover the identity of a defendant is warranted.” *Columbia Ins. Co. v. seescandy.com*,
12 185 F.R.D. 573, 578 (N.D. Cal. 1999). Such early discovery should be limited “to ensure
13 that this unusual procedure will only be employed in cases where the plaintiff has in good
14 faith exhausted traditional avenues for identifying a civil defendant pre-service” and to
15 “prevent use of this method to harass or intimidate.” *Id.* “First, the plaintiff should identify
16 the missing party with sufficient specificity such that the Court can determine that
17 defendant is a real person or entity who could be sued in federal court.” *Id.* Second, the
18 plaintiff “should identify all previous steps taken to locate the elusive defendant” to ensure
19 that the plaintiff has made a good faith effort to identify and serve process on the defendant.
20 *Id.* at 579. Third, the “plaintiff should establish to the Court’s satisfaction that plaintiff’s
21 suit against defendant could withstand a motion to dismiss.” *Id.* “Thus, plaintiff must
22 make some showing that an act giving rise to civil liability actually occurred and that the
23 discovery is aimed at revealing specific identifying features of the person or entity who
24 committed that act.” *Id.* at 580.

25 “Lastly, the plaintiff should file a request for discovery with the Court, along with a
26 statement of reasons justifying the specific discovery requested as well as identification of
27 a limited number of persons or entities on whom discovery process might be served and
28

1 for which there is a reasonable likelihood that the discovery process will lead to identifying
2 information about defendant that would make service of process possible.” *Id.*

3 **A. Identification of the Defendant with Sufficient Specificity.**

4 In support of the *Ex Parte* Application, plaintiff submitted three relevant
5 declarations. First, a Declaration by Tobias Fieser states that he is employed by IPP
6 International UG (IPP), which provides forensic investigation services to copyright owners
7 by tracking, monitoring, and detecting copyright infringement over the internet. [Doc. No.
8 4-2, at p. 11.] According to Mr. Fieser, IPP monitors the BitTorrent file distribution
9 network for the presence of plaintiff’s copyrighted works. [Doc. No. 4-2, at p. 11.] Based
10 on his review of forensic activity records and other forensic evidence, Mr. Fieser states that
11 he was able to determine that IP address 99.26.127.96 was used to distribute “multiple
12 pieces” of plaintiff’s copyrighted movies. [Doc. No. 4-2, at p. 11.] Each of these pieces
13 was recorded in digital files that are identified by a “Cryptographic Hash Value.” [Doc.
14 No. 4-2, at p. 12.] Software was then used to re-assemble and analyze the digital files to
15 confirm that the files being distributed by defendant’s IP address were pieces of plaintiff’s
16 copyrighted movies that were “fully playable.” [Doc. No. 4-2, at p. 12.] According to
17 Mr. Fieser’s Declaration, Exhibit A to the Complaint [Doc. No. 1-2, at pp. 1-9] lists digital
18 files of plaintiff’s copyrighted works that were distributed using the defendant’s IP address.
19 [Doc. No. 4-2, at p. 12.]

20 Second, a Declaration by Susan B. Stalzer states that she is plaintiff’s employee and
21 is familiar with plaintiff’s copyrighted movies. She was charged with reviewing the digital
22 files enumerated on Exhibit A that were collected by IPP during its forensic investigation
23 to verify that the files did indeed contain plaintiff’s copyrighted movies. Following this
24 verification process, she used the American Registry for Internet Numbers (ARIN) to
25 confirm that defendant’s IP address was owned by AT&T U-verse at the times of the
26 alleged infringements. [Doc. No. 4-2, at pp. 19-20.]

27 Third, a Declaration by Philip Pasquale states that he is a tech advisor for a firm that
28 specializes in network security, data breaches, and the protection of secured information

1 transmitted across networks. [Doc. No. 4-2, at p. 15.] Mr. Pasquale was retained by
2 plaintiff “to individually analyze and retain forensic evidence captured by IPP. . . .” [Doc.
3 No. 4-2, at p. 15.] He used a program called Wireshark to review the contents of the digital
4 files collected by IPP and was able to confirm a “transaction with 99.26.127.96 at
5 10/18/2018 04:17:22 UTC.” [Doc. No. 4-2, at p. 15.] Based on his experience in other
6 cases, Mr. Pasquale also represents that AT&T U-verse is the “only entity that can correlate
7 the IP address to its subscriber and identify defendant as the person assigned the IP address
8 99.26.127.96 during the time of the alleged infringement.” [Doc. No. 4-2, at pp. 15-16.]

9 The Complaint also alleges that geolocation technology by Maxmind Inc., “an
10 industry-leading provider of IP address intelligence and online fraud detection tools,” was
11 used to determine that “defendant’s IP address traced to a physical address in this District.”
12 [Doc. No. 1, at p. 2-3. *See also* Doc. No. 4-1, at pp. 12-13.] In this regard, the Complaint
13 also states as follows: “In order to ensure that defendant’s IP address accurately traced to
14 the District, plaintiff inputted defendant’s IP address into Maxmind’s GeoIP database
15 twice: first when it learned of the infringement and again, just prior to filing this lawsuit.”
16 [Doc. No. 1, at p. 3.]

17 “Some district courts in the Ninth Circuit have determined that a plaintiff identifies
18 Doe defendants with sufficient specificity by providing the unique IP address assigned to
19 an individual defendant on the day of the alleged infringing conduct, and by using
20 ‘geolocation technology’ to trace the IP address to a physical point of origin.” *See, e.g.,*
21 *Malibu Media, LLC v. Does 1-19*, 2012 WL 2152061, at 3 (S.D. Cal. June 12, 2012), and
22 cases cited therein. Here, without explanation, plaintiff did not submit a declaration
23 supporting its assertion that geolocation technology was used to ensure that the subscriber
24 of the subject IP address was located in this District during the time of the alleged
25 infringement.

26 ***B. Previous Steps Taken to Identify Defendant.***

27 In its *Ex Parte* Application, defendant has represented that it has consulted with
28 computer investigators and cyber security consultants and has searched sources available

1 to the public but is unable to obtain the name and address of the subscriber of IP address
2 99.26.127.96 for the time period in question. [Doc. No. 4-1, at pp. 13-14.] Through
3 publicly available data, plaintiff is only able to connect IP address 99.26.127.96 to
4 infringing activity on specified dates and identify the specific ISP associated with that IP
5 address. [Doc. No. 4-1, at pp. 13-14.] Without a subpoena to the ISP requesting the name
6 and address of the subscriber to the IP address in question, plaintiff will be unable to
7 identify and serve defendant. [Doc. No. 4-1, at p. 17.]

8 The Court is also aware that the requirements of the Cable Privacy Act, 47 U.S.C.
9 § 551, generally prohibit cable operators from disclosing personally identifiable
10 information regarding subscribers without the prior written or electronic consent of the
11 subscriber. 47 U.S.C. § 551(c)(1). A cable operator, however, may disclose such
12 information if the disclosure is made pursuant to a court order, and the cable operator
13 provides the subscriber with notice of the order. 47 U.S.C. § 551(c)(2)(B). Therefore, the
14 information plaintiff seeks pursuant to a subpoena falls within an exception to the
15 prohibition on disclosure within the Act.

16 Accordingly, based on the information provided in the *Ex Parte* Application and
17 supporting Declarations, the Court finds that plaintiff did make a good faith effort to
18 identify and serve the defendant but is unable to do so without an Order from the Court
19 allowing service of a subpoena on the ISP associated with the IP address in question.

20 **C. Ability to Withstand a Motion to Dismiss.**

21 Under Federal Rule of Civil Procedure 12(b), a case can be dismissed for lack of
22 subject matter jurisdiction or for failure to state a claim upon which relief can be granted.
23 Fed.R.Civ.P. 12(b)(1), 12(b)(6). “Under the Copyright Act of 1976 (‘the Act’) a plaintiff
24 may not ‘institute []’ an action in federal district court ‘until registration of the copyright
25 claim has been made in accordance with this title.’ 17 U.S.C. § 411(a).” *Berry v. Penguin*
26 *Group (USA), Inc.*, 448 F.Supp.2d 1202, 1202 (W.D. Wash. 2006). In order to state a
27 viable claim for copyright infringement, a plaintiff must allege: (1) ownership of a valid
28 copyright, and (2) a violation by the defendant of the copyright owner’s exclusive rights

1 under the Copyright Act. *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004); 17
2 U.S.C. § 501(a).

3 As applied herein, the Complaint adequately alleges subject matter jurisdiction
4 pursuant to Title 28, United Code, Sections 1331 (federal question) and 1338 (copyrights).
5 The Complaint further alleges that plaintiff is either the registered owner or has pending
6 registration applications for the adult motion pictures that defendant's IP address copied
7 and distributed using the BitTorrent file distribution network without plaintiff's
8 authorization. [Doc. No. 1 at pp. 1, 6]. Thus, it is apparent that plaintiff's Complaint could
9 withstand a motion to dismiss for failure to state a claim.

10 Under Federal Rule of Civil Procedure 12(b), a complaint can also be dismissed for
11 lack of personal jurisdiction over a defendant or for improper venue. Fed.R.Civ.P.
12 12(b)(2)&(3). To overcome a defendant's motion to dismiss under Federal Rule 12(b)(2)
13 for lack of personal jurisdiction, a plaintiff need only make a *prima facie* showing of
14 jurisdiction by presenting facts that, if true, would support a finding of personal jurisdiction
15 over the defendant. *Ballard v. Savage*, 65 F.3d 1495, 1498 (9th Cir. 1995). Personal
16 jurisdiction can be established over a person who resides in the forum state. *Brayton*
17 *Purcell LLP v. Recordon & Recordon*, 361 F.Supp.2d 1135, 1138 (N.D. Cal. 2005). In
18 copyright infringement actions, venue is proper "in the district in which the defendant . . .
19 resides or may be found." 28 U.S.C. § 1400(a).

20 Based on the record before the Court, plaintiff has not satisfied its burden to make a
21 *prima facie* showing that the Complaint is likely to survive a motion to dismiss for lack of
22 personal jurisdiction and/or improper venue. First, the Complaint alleges that geolocation
23 technology was used to trace the offending IP address to a location in this District. Second,
24 the Complaint alleges that the defendant resides here based on the results of geolocation
25 technology. Third, the Complaint asserts that a substantial part of the alleged copyright
26 infringement occurred in this District. However, plaintiff did not submit evidence to
27 support these allegations. As a result, this Court cannot conclude plaintiff met its burden
28 of making a *prima facie* showing that the Complaint would be able to survive a motion to

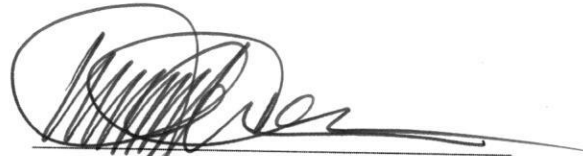
1 dismiss for lack of personal jurisdiction and/or improper venue. Without supporting
2 evidence indicating the offending IP address was located within this District during the
3 relevant time period, the Court finds that it would not be appropriate to permit plaintiff to
4 serve AT&T Inc and/or AT&T U-verse with a Rule 45 subpoena.

5 **CONCLUSION**

6 For the reasons set forth above, plaintiff's *Ex Parte* Application for Leave to Serve
7 a Third Party Subpoena is DENIED without prejudice. [Doc. No. 4.] No later than ten
8 (10) days from the date this Order is entered, plaintiff may file competent evidence based
9 on personal knowledge that a reliable geolocation service was used to determine that the
10 subject IP address was located within the Southern District of California during the relevant
11 time period.

12 **IT IS SO ORDERED.**

13 Dated: March 21, 2019



14
15 Hon. Karen S. Crawford
16 United States Magistrate Judge
17
18
19
20
21
22
23
24
25
26
27
28