

United States District Court

1 2

### BACKGROUND

Plaintiff is an individual doing business as Axel Braun Productions, which produces
adult entertainment products. (Dkt. No. 1 ¶¶ 9-10.) Plaintiff directed the video at issue – *Star Wars XXX: A Porn Parody* – which was produced by Axel Braun Productions and Vivid
Entertainment, LLC. (Dkt. No. 4-1 ¶ 3.) The video was registered with the Copyright Office
on February 21, 2012 in the name of Vivid Entertainment LLC & Axel Braun Productions.
(Dkt. No. 4-2, Ex. A.)

Plaintiff alleges that Primary Distributor Doe Number One and Does Two through
Sixty-Nine (collectively "Defendants") used BitTorrent, an internet peer-to-peer ("P2P") file
sharing network, to illegally reproduce and distribute Plaintiff's copyrighted work in violation
of the Copyright Act, 17 U.S.C. § 101 et seq. (Dkt. No. 1 ¶¶ 31-35.) Plaintiff further alleges
that by using the BitTorrent program to download and distribute Plaintiff's content, each
Defendant engaged in contributory infringement and is jointly and severally liable. (Id. at ¶¶
36-45.)

The process by which file sharing occurs begins with P2P networks which are "computer systems that enable Internet users to make files on their computers available to others, search for files stored on other users' computers, and transfer exact copies of files from one computer to another via the Internet." (Dkt. No. 4-1¶ 7.) BitTorrent is a P2P network which allows "small computers with low bandwidths" to participate in "large data transfers across a P2P network." (Id.) This process plays out as follows:

in a process called "seeding" an initial file-provider shares a file with P2P networks. Other users ("peers") on the network connect to the seed file to download. Each new file downloader receives a different piece of data from each user who has already downloaded the file that together comprises the whole. This piecemeal system with multiple pieces of data coming from different peer members is called a "swarm." As new peers request the same file, each new peer becomes a part of the network and the peers offer parts of the file stored on their computers to other peers. This means that every "node" or peer who has a copy of the infringing copyrighted material also becomes a source of download for that infringing file.

 $_{28}$  (Dkt. No. 4-1 ¶ 8.)

United States District Court Northern District of California

21

22

23

24

25

26

11

12

13

14

15

16

17

18

19

28

Plaintiff retained the services of Media Protector International GmbH ("MPI"), a 1 2 technology company that specializing in P2P content detection and user identification to 3 locate infringing copies of Plaintiff's works on P2P networks. (Dkt. No. 4-1 ¶ 2.) MPI was 4 able to identify and document internet protocol ("IP") addresses from which individuals connected to the Internet, as well as the date and time the individuals used the IP addresses to 5 share files on the P2P network. (Dkt. No. 4 at 11:1-12.) MPI determined that from 9:55 a.m. 6 on April 1, 2012 to 10:13 p.m. on April 2, 2012, Doe One offered pieces of Plaintiff's 7 copyrighted work to other peers and Does Two through Sixty-Nine downloaded pieces of that 8 file and engaged in simultaneous redistribution over the P2P network. (Dkt. No. 4-1 at Ex. 9 A.) 10

Because Defendants' conduct occurred behind the mask of their anonymous IP addresses, Plaintiff cannot identify the Defendants without leave to subpoena Defendants' internet service providers ("ISPs") for the identity of the individual or entity related to each IP address. Based on the information obtained by MPI, including the specific date and time of download, Plaintiff alleges that the ISPs will be able to identify the name and address of each Doe Defendant. (Dkt. No. 4 at 11:12-14.) Consequently, Plaintiff asks the Court to grant expedited discovery to issue subpoenas to the relevant ISPs to require the ISPs to disclose the name, address, telephone number, and email address for each of Defendant's IP address.

## DISCUSSION

Federal Rule of Civil Procedure 26(d)(1) prohibits discovery without a court order prior to a Rule 26(f) conference between the parties. Courts generally use a "good cause" standard to decide whether to permit such early discovery. <u>Semitool, Inc. v. Tokyo Electron</u> <u>America, Inc.</u>, 208 F.R.D. 273, 276 (N.D. Cal. 2002). "Good cause may be found where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice of the responding party." Id. at 276.

To determine whether there is "good cause" to permit expedited discovery to identify anonymous internet user doe defendants, courts consider whether:

(1) the plaintiff can identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could

United States District Court Northern District of California locate the elusive defendant; (3) the plaintiff's suit against defendant could withstand a motion to dismiss; and (4) the plaintiff has demonstrated that there is a reasonable likelihood of being able to identify the defendant through discovery such that service of process would be possible.
<u>OpenMind Solutions, Inc. v. Does 1-39</u>, No. 11–3311, 2011 WL 4715200, at \*2 (N.D. Cal. Oct. 7, 2011) citing Columbia Ins. Co. v. seescandy. com, 185 F.R.D. 573, 578–80 (N.D. Cal.

1999). The Court will consider each of these factors in turn.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

# A. Identification of Defendants as Persons Who Can Be Sued

be sued in federal court; (2) the plaintiff has identified all previous steps taken to

Plaintiff has satisfied the first factor: whether Plaintiff has identified the Doe Defendants with sufficient specificity such that the Court can conclude that each Defendant is a real person or entity that would be subject to the Court's jurisdiction. First, Plaintiff represents that he has taken steps to ensure that the IP addresses accurately reflect addresses that were used to copy Plaintiff's copyrighted work. Second, Plaintiff also represents that he has used geolocation technology to trace the IP addresses of each Doe Defendant to California; in other words, Plaintiff has made a prima facie showing of personal jurisdiction over each Doe Defendant. <u>See DigiProtect USA Corp. v. Does</u>, 2011 WL 4444666 at \*1 (S.D.N.Y. Sep. 26, 2011) (stating that "[p]ublicly available software provides basic, or at least presumptive, geographic information about IP addresses").

# B. <u>Previous Steps Taken to Identify the Doe Defendants</u>

With respect to the second factor, Plaintiff has also identified the specific steps he has taken to identify the Doe Defendants and explained why he is unable to name and serve them at this time. <u>Columbia Ins. Co.</u>, 185 F.R.D. at 579. As the Doe Defendants accessed Plaintiff's video via the Internet without any identifying information other than their unique IP addresses, Plaintiff is unable to further identify the Defendants without information from the ISPs.

25

# C. <u>Withstanding a Motion to Dismiss</u>

The Court also concludes that Plaintiff has made a prima facie showing that the
 Complaint would withstand a motion to dismiss. To prevail on his copyright claim, Plaintiff
 must prove (1) that it owns a valid copyright, and (2) that each defendant copied a work

covered by the copyright. Online Policy Group v. Diebold, Inc., 337 F.Supp.2d 1195, 1199 1 (N.D. Cal. Sep. 30, 2004). "To be liable for direct infringement, one must actively engage in 2 and directly cause the copying." Id. (internal quotation marks and citation omitted). Plaintiff 3 4 has submitted evidence that his company is a co-claimant of the copyright for the video at issue. And he has alleged how and when each Doe Defendant intentionally copied the work, 5 and has explained how he determined each identified IP address. 6

Plaintiff has also made a prima facie showing that the Complaint would withstand a 7 motion to dismiss for lack of personal jurisdiction. The Complaint alleges that the ISP 8 associated with each Doe Defendant is located in California; thus, the allegations of the 9 Complaint support an inference that all of the Doe Defendants reside in California. At this 10 stage in the proceedings, this is a sufficient showing. 11

Another issue frequently addressed by courts in these types of cases is whether the Doe 12 Defendants are properly joined. Federal Rule of Civil Procedure 20 permits joinder of 13 defendants in a single action if a right to relief is asserted against them "arising out of the 14 same transaction, occurrence, or series of transactions or occurrences" and a "question of law 15 or fact common to all defendants will arise in the action." Fed. R. Civ. P. 20(a)(2)(A)(B). 16 "[T]he impulse is toward entertaining the broadest possible scope of the action consistent with fairness to the parties; joinder of claims, parties and remedies is strongly encouraged." 18 United Mine Workers of America v. Gibbs, 383 U.S. 715, 724 (1966); see also League to 19 Save Lake Tahoe Reg'l Planning Agency, 558 F.2d 914, 917 (9th Cir. 1997) (stating that the 20 "primary purpose" of Rule 20 "is to promote trial convenience and to prevent multiple 21 lawsuits"). 22

Plaintiff asserts that because all of the Doe Defendants were part of the same swarm 23 downloading and distributing the same Star Wars XXX: A Porn Parody file during a limited 24 thirty-six hour period of time, the copyright claims arise from the same transaction and 25 occurrence and raise common issues of law and fact. While several courts have concluded 26 that joinder is inappropriate under similar circumstances, see, e.g., Hard Drive Productions, 27 Inc. v. Does 1-130, 2011 WL 5573960 (N.D. Cal. Nov. 16, 2011), the Court concludes that 28

17

Plaintiff has at least made a prima facie showing that the Doe Defendants are properly joined. 1 2 See OpenMind Solutions, Inc., 2011 WL 4715200 at \*7 (concluding that plaintiff made a 3 preliminary showing that satisfied Rule 20 given the allegations that the doe defendants were 4 present in the same BitTorrent swarm and shared pieces of the same seed file). As the case progresses, the Court may conclude that it is unmanageable, depending on the number of 5 defendants served and appearing, or that, in fact, the claims do not arise from the same 6 transaction and occurrence. At this time, however, the Court is not persuaded that Plaintiff 7 could not withstand a motion to dismiss for improper joinder. 8

9

10

11

12

13

14

15

16

17

19

21

23

#### D. Likelihood of Identifying the Doe Defendants Through Discovery

The final factor concerns whether the discovery sought will uncover the identities of the Doe Defendants. See Gillespie v. Civiletti, 629 F.2d 637, 642-43 (9th Cir. 1980) (stating that early discovery to identify doe defendants should be allowed "unless it is clear that discovery would not uncover the identities"); Wakefield v. Thompson, 177 F.3d 1160, 1163 (9th Cir. 1999) (holding that "the plaintiff should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities").

Here, this is a multi-step process. ISPs assign a unique IP address to each subscriber and retain subscriber activity records regarding the IP addresses assigned; thus, the 18 information subpoenaed will reveal the name and contact information of the subscriber to the Internet connection that was used to download the copyrighted work, but it will not reveal 20 who actually downloaded the work and therefore who can be named as a defendant. The Internet connection could have been used by the subscriber, by another member of the 22 household, by a visitor to the household, or by someone secretly using an unsecure connection. 24

Plaintiff has proposed the following safeguards to protect the due process rights of 25 these subscribers. First, upon receipt of the subpoena, the ISP shall provide the individual 26 subscribers with a copy of the subpoena and a copy of this Order. The subscribers will then 27 have thirty days to file a motion in this Court regarding the subpoenas, and only if the thirty-28

day period passes without the subscriber contesting the subpoena shall the ISP provide the
information responsive to the subpoena to Plaintiff. (Dkt. No. 4 p. 28-29.) Once identified,
Plaintiff suggests that some of the Doe Defendants will likely be dismissed because Plaintiff
cannot locate them, there are extenuating circumstances (presumably including the fact that
that the subscriber was not the individual who allegedly downloaded the copyrighted work),
or because the parties settle their claims without further litigation. (Dkt. No. 4 20:6-19.)

Given the foregoing, the Court concludes that it is not clear that requested early 7 discovery, namely the subpoenas to the ISPs, will not lead to the discovery of the identities of 8 the Doe Defendants. The Court recognizes that before granting such discovery it must weigh 9 any prejudice to the responding party. In these circumstances, where Plaintiff has a good 10 faith belief that the Doe Defendants reside in California, has submitted declarations outlining 11 the steps it has taken to ensure that the identified Doe Defendants in fact downloaded 12 Plaintiff's copyrighted material, and has limited its case to a narrow period of time, the Court 13 concludes that good cause has been shown. 14

#### CONCLUSION

For the reasons stated above, the Court GRANTS Plaintiff's Ex Parte Application for Expedited Discovery (Dkt. No. 4) as follows:

Plaintiff is allowed to serve immediate discovery on Does 1–69's ISPs listed in
Exhibit A to the Declaration of Michael Eichner (Dkt. No. 4-1) by serving a Rule 45
subpoena that seeks information sufficient to identify the Doe Defendants, including the name
and address of Does 1–69. Plaintiff's counsel shall issue the subpoena and attach a copy of
this Order.

Each ISP will have 20 days from the date of service upon it to serve Does 1–69 with a copy of the subpoena and a copy of this Order. The ISPs may serve the Doe Defendants using any reasonable means, including written notice sent to his or her last known address, transmitted either by first-class mail or via overnight service.

Does 1–69 shall have 30 days from the date of service upon him, her, or it to file any motions in this Court contesting the subpoena (including a motion to quash or modify the

15

16

subpoena). If that 30-day period lapses without Does 1-69 contesting the subpoena, the ISP 1 2 shall have 14 days to produce the information responsive to the subpoena to Plaintiff.

3 Because no appearance by a person at a deposition is required by the subpoena, instead 4 only production of documents, records and the like is required, the witness and mileage fees required by Rule 45(b)(1) of the Federal Rules of Civil Procedure do not apply and no such 5 fees need be tendered. 6

The subpoenaed entity shall preserve all subpoenaed information pending the ISP's delivering such information to Plaintiff or the final resolution of a timely filed and granted motion to quash the subpoena with respect to such information.

Any information disclosed to Plaintiff in response to a subpoena may be used by 10 Plaintiff solely for the purpose of protecting its rights under the Copyright Act, 17 U.S.C. §§ 101–1322. 12

Plaintiff shall serve each Doe Defendant with the summons, complaint, and other documents required by Civil Local Rule 4–2 within 120 days of learning that Doe's identity.

Should Plaintiff engage in settlement negotiations with any Doe Defendant, it shall not assert that that Doe is being sued in San Francisco, unless Plaintiff believes that Doe to be a resident of this District or has a good faith belief, consistent with Federal Rule of Civil Procedure 11(b), that it can otherwise establish personal jurisdiction over that Doe in this District.

**IT IS SO ORDERED.** 

Dated: August 21, 2012 22

acqueline S.Co

T CORLEY UNITED STATES MAGISTRATE JUDGE

Northern District of California United States District Court

7

8

9

11

13

14

15

16

17

18

19

20

21

23

24

25

26

27