E-FILED 08-02-2011

NOT FOR CITATION

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

AF HOLDINGS LLC.,

Plaintiff,

v.

DOES 1-135,

Defendants.
_____/

No. C11-03336 JF (HRL)

ORDER GRANTING PLAINTIFF'S EX PARTE APPLICATION FOR LEAVE TO TAKE LIMITED EXPEDITED DISCOVERY

[Re: Docket No. 8]

BACKGROUND

Plaintiff AF Holdings LLC ("AFH"), a company based in the Federation of Saint Kitts and Nevis, filed this complaint on July 7, 2011. AFH alleges that at least one hundred and thirty-five unknown Defendants knowingly and willfully infringed its copyright by downloading and sharing its copyrighted work ("Work"). Specifically, AFH alleges that Doe Defendants engaged in unlawful concerted conduct for the purpose of infringing its Work using an online peer-to-peer ("P2P") file-sharing tool called BitTorrent, in violation of the Copyright Act, 17 U.S.C. § 101 *et seq*. See Compl. at 4-6. The BitTorrent protocol, as explained by Judge Grewal:

> is a decentralized method of distributing data. Since its release approximately 10 years ago, BitTorrent has allowed users to share files anonymously with other users. Instead of relying on a central server to distribute data directly to individual users, the BitTorrent protocol allows individual users to distribute data amo[ng] themselves by exchanging pieces of the file with each other to eventually obtain a whole copy of the file. When using the BitTorrent protocol, every user simultaneously receives information from and transfers information to one another.

> In the BitTorrent vernacular, individual downloaders/distributors of a particular file are called "peers." The group of peers involved in downloading/distributing a particular file is called a "swarm." A server which stores a list of peers in a swarm is called a "tracker." A computer program that implements the BitTorrent protocol is called a BitTorrent "client."
>
> The BitTorrent protocol operates as follows. First, a user locates a small "torrent" file. This file contains information about the files to be shared and about the tracker, the computer that coordinates the file distribution. Second, the user loads the torrent file into a BitTorrent client, which automatically attempts to connect to the tracker listed in the torrent file. Third, the tracker responds with a list of peers and the BitTorrent client connects to those peers to begin downloading data from and distributing data to the other peers in the swarm. When the download is complete, the BitTorrent client continues distributing data to the peers in the swarm until the user manually disconnects [from] the swarm or the BitTorrent client otherwise does the same.

Diabolic Video Productions, Inc. v. Does 1-2099, No. 10-CV-5865 (PSG), 2011 U.S. Dist. LEXIS 58351, at *3-4 (N.D. Cal. May 31, 2011). As AFH notes, the BitTorrent protocol "necessitates concerted action by many people in order to disseminate files" without which it is "impossible" for users to download files. Compl. at 3:5-9. As each new peer joins a swarm and begins to download and share the designated file, the swarm grows larger and gains greater efficiency. See Hansmeier Decl. at ¶ 7. BitTorrent also allows users to exchange files without having to disclose their identities, using only an Internet Protocol ("IP") address assigned to them by their respective Internet Service Providers ("ISP"). See Compl. at 4.

AFH hired Media Copyright Group ("MCG"), a firm specializing in online piracy detection, to identify the IP addresses of individuals engaged in file-sharing of its copyrighted Work. See Hansmeier Decl. at ¶¶ 12-20. MCG used proprietary forensic software to locate the swarms downloading and distributing AFH's Work and to identify the IP address of each user in the swarm, noting the date and time of the observed activity. See id., Compl. Ex. A.

AFH joined multiple Doe Defendants in this suit, claiming that P2P sharing of its copyrighted Work comprised a transaction or series of transactions and asserting common questions of law and fact among each Defendant. See Compl. at 3. Using the list of IP addresses, AFH seeks leave to subpoena the ISPs to identify each Doe Defendant's name, address, telephone number, email address, and Media Access Control information. Application at 24:6-16. AFH claims that it cannot identify Doe Defendants for purposes of service of

process unless its Ex Parte Application for Leave to Take Limited Expedited Discovery ("Application") is granted.

LEGAL STANDARD

Under Federal Rule of Civil Procedure 26(d), a court may authorize early discovery before the Rule 26(f) conference for the parties' convenience and in the interest of justice. FED. R. CIV. P. 26(f)(1), (2). Courts within the Ninth Circuit generally use a "good cause" standard to determine whether to permit such discovery. See, e.g., Apple Inc. v. Samsung Electronics Co., Ltd., No. 11–CV–01846 LHK, 2011 WL 1938154, at *1 (N.D. Cal. May 18, 2011); Semitool, Inc. v. Tokyo Electron America, Inc., 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 to the responding party." Semitool, 208 F.R.D. at 276.

While discovery normally only takes place after a defendant has been served, where the alleged tortious activity occurs entirely on-line, "[s]ervice of process can pose a special dilemma for plaintiffs ... because the defendant may have used a fictitious name and address in the commission of the tortious acts." Liberty Media Holdings, LLC v. Does 1-62, No. 11-CV-575 MMA (NLS), 2011 WL 1869923, at *2 (S.D. Cal. May 12, 2011) (quoting Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 577 (N.D. Cal. 1999)). In determining whether there is good cause to allow expedited discovery to identify anonymous Internet users named as 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 be sued in federal court; (2) the plaintiff has identified all previous steps taken to 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. Seescandy.com, 185 F.R.D. at 578-80.

DISCUSSION

AFH has met its burden as set forth above. First, AFH's agent MCG used its forensic

software to identify the unique IP addresses of individuals engaged in P2P sharing of the Work, noting the date and time of this activity. See Hansmeier Decl. at ¶¶ 15. The forensic analysis included verification of each IP address to ensure that it corresponded to users who actually reproduced and distributed the Work. See id. at ¶¶ 18-20. Plaintiff also used "geolocation" technology to trace these IP addresses to a point of origin within the state of California. Compl. at ¶ 3. AFH has sufficiently shown that Doe Defendants are real persons likely residing in California who may be sued in this Court.

Second, AFH has taken reasonable steps to identify these Doe Defendants but has been unable to do so. MCG's investigation revealed only the IP addresses of Doe Defendants and their affiliated ISPs, noting the date and time of the observed activity. See Hansmeier Decl. at ¶¶ 15-18. AFH asserts that it has exhausted all other means of identifying Doe Defendants and that ultimate identification depends on a court order authorizing a subpoena of the ISPs. See Hansmeier Decl. at ¶ 21.

Third, this court is satisfied that AFH's complaint would likely withstand a motion to dismiss. AFH has sufficiently pled a prima facie case of copyright infringement under the Copyright Act, 17 U.S.C. § 101 *et seq*., and Doe Defendants, having engaged in the same transaction or series of transactions, share common questions of law and fact and are thus properly joined.

Fourth, AFH has shown that there is a reasonable likelihood that its requested discovery will lead to the identification of Doe Defendants. AFH asserts that ISPs assign a unique IP address to individual users and that an ISP retains records pertaining to those IP addresses for a limited period of time. Hansmeier Decl. at ¶¶ 16-17.

CONCLUSION

Based on the foregoing, the Court GRANTS AFH's motion for expedited discovery. Accordingly, IT IS ORDERED THAT:

1. AFH may immediately serve Rule 45 subpoenas on the ISPs listed in Exhibit A to the Complaint to obtain information that will identify each Doe Defendant, including name, address, telephone number, email address, and media access

control information. Each subpoena shall have a copy of this Order attached.

2. Each ISP will have 30 days from the date of service upon them to serve the subscribers of the IP addresses with a copy of the subpoena and a copy of this order. The ISPs may serve the subscribers using any reasonable means, including written notice sent to the subscriber's last known address, transmitted either by first-class mail or via overnight service.

3. Subscribers shall have 30 days from the date of service upon them to file any motions in this court contesting the subpoena (including a motion to quash or modify the subpoena). If that 30–day period lapses without a subscriber contesting the subpoena, the ISPs shall have 10 days to produce the information responsive to the subpoena to AFH.

4. The subpoenaed entity shall preserve any subpoenaed information pending the resolution of any timely-filed motion to quash.

5. Any ISP that receives a subpoena pursuant to this Order shall confer with AFH and shall not assess any charge in advance of providing the information requested in the subpoena. Any ISP that receives a subpoena and elects to charge for the costs of production shall provide AFH with a billing summary and cost reports that serve as a basis for such billing summary and any costs claimed by such ISP.

6. AFH shall serve a copy of this order along with any subpoenas issued pursuant to this order to the necessary entities.

7. Any information disclosed to AFH in response to a Rule 45 subpoena may be used by AFH solely for the purpose of protecting its rights as set forth in its complaint.

IT IS SO ORDERED.

DATED: August 2, 2011

HOWARD R. LLOYD
UNITED STATES MAGISTRATE JUDGE

5:11-cv-03336-JF Notice has been electronically mailed to:

Brett Langdon Gibbs blgibbs@wefightpiracy.com

Counsel are responsible for distributing copies of this document to co-counsel who have not registered for e-filing under the court's CM/ECF program.