UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

MALIBU MEDIA, LLC,

Plaintiff,

v.

JOHN DOE subscriber assigned IP address 68.32.2.28,

Defendant.
_____ /

Case No. 17-10432

District Judge Sean F. Cox

Magistrate Judge R. Steven Whalen

OPINION AND ORDER

This is a copyright infringement case. Plaintiff Malibu Media, LLC ("Malibu") owns copyrights to various films, including 13 specific copyrighted works that are the subject of this lawsuit. *See Complaint* [Doc. #1], Exhibit B. Before the Court is Malibu's motion for leave to serve a third party subpoena on Internet Service Provider Comcast Cable ("Comcast") prior to a Rule 26(f) conference [Doc. #2].[1] For the reasons discussed below, the motion is GRANTED.

Malibu does not know the name of the John Doe Defendant, but states that it has identified the Defendant by a unique Internet Protocol ("IP") address that was involved in the alleged infringement (i.e., downloading a movie without paying) while participating in a "BitTorrent swarm."[2]

[1] The brief support of this motion is filed under Doc. #3.

[2] In *Third Degree Films v. Does 1-36*, 2012 WL 2522151, *1 -2 (E.D.Mich. 2012), Judge Michelson explained the BitTorrent protocol as follows:

> "Although it may be used for improper purposes, the BitTorrent communication protocol itself is not without ingenuity. File sharing, as relevant here, involves the challenge of quickly distributing copies of a large digital file, e.g., a digital movie file like those found on a DVD, to a

large number of people. Under more traditional file-sharing approaches, a digital file might reside on a few computers, e.g., servers, and those interested in the file would download a copy of the file from those limited sources. But, because these files tend to be large, and, perhaps, in high demand, a high load is placed on these limited source computers and their associated internet bandwidth. Thus, distribution to this so-called "flash crowd" may be slow.

"BitTorrent is one of several peer-to-peer file sharing protocols that address the inefficiencies in the client-server model by making those who download a file another source for the file. That is, sharing is among "peers." Users of the BitTorrent communication protocol also do not have to download an entire file before uploading parts of the file to others. This is because BitTorrent downloads a file in pieces, and by default, begins sharing pieces with other peers almost immediately. More specifically, the file distribution process using the BitTorrent protocol works as follows. Initially, an individual with BitTorrent software obtains a copy (perhaps legally) of the large digital file he wishes to share (in this case, a digital version of the Work). This individual, known in BitTorrent parlance as the "initial seeder," uses his BitTorrent software to divide the large file into thousands of smaller digital files known as "pieces." The software also creates a unique "digital fingerprint," a 40 character alpha-numeric code, for each piece. The initial seeder's BitTorrent software also creates an associated ".torrent" file which includes information about the original digital file, the pieces, and each piece's digital fingerprint. The initial seeder then posts this .torrent file—but not the large digital file to which it corresponds—to one of various websites on the internet that host .torrent files.

"When a BitTorrent user is interested in obtaining a copy of a particular digital file, e.g., the digital movie file at issue in this case, he can search the internet, perhaps using one of several torrent search engines, to find a . torrent file associated with the digital file of interest. Once a user downloads this .torrent file, the BitTorrent software, with the help of another internet-connected computer running BitTorrent software known as a "tracker," uses the information in the .torrent file to locate a "swarm" of peers sharing pieces of the particular digital file described by the .torrent file. Downloads may be from any peer that has already downloaded a piece of the particular digital file. This is possible because the BitTorrent software, by default, offers for download any piece of a digital file that it has previously downloaded. When a peer has copied a piece from another peer, the BitTorrent software verifies the authenticity of the piece by checking its digital fingerprint; once this is done, the peer becomes another source for that piece. Although a particular BitTorrent swarm may, over its lifetime, consist of thousands of peers, at any given moment each peer is only directly sharing with a small fraction of the swarm. Once a peer has downloaded all the pieces of the digital file of interest (possibly receiving pieces from dozens of different peers), the BitTorrent software re-assembles

Plaintiff has proffered the declaration of Tobias Feiser of IPP, Limited ("IPP"), a company that provides forensic investigation services to copyright owners. Mr. Feiser states that as part of his duties, he monitors the BitTorrent file distribution network for the presence of copyrighted works, and "identif[ies] the Internet Protocol ("IP") addresses that are being used by infringers to distribute these copyrighted works." *Feiser Declaration*, ¶6 [Doc. #4]. Mr. Feiser states that as part of his investigation, he found that a person using Defendant's IP address engaged in BitTorrent transactions with regard to the copyrighted works alleged in the complaint. *Id*. ¶¶ 8-13.

F. R. Civ. P. 26(d)(1) provides: "A party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except in a proceeding exempted from initial disclosure under Rule)(1)(B), or when authorized by these rules, by stipulation, *or by court order"* (emphasis added). Malibu is correct that a district court has the discretion to permit the early issuance of a Rule 45 subpoena prior to a Rule 26(f) conference. This issue arises not infrequently in copyright infringement cases where the identity of the alleged infringer is not known. *See Arista Records, LLC v. Doe 3*, 604 F.3d 110 (2nd Cir. 2012). The standard for granting a motion for this type of subpoena is good cause. *Id*. The factors that a court considers are (1) a prima facie showing of copyright infringement, (2) a specific discovery request, (3) an absence of alternative means to obtained the subpoenaed information, (4) plaintiff's central need for the subpoenaed information, and (5) the defendant's minimal expectation of privacy. *Id*.

---

the pieces to a single digital (movie) file. The file is then usable, or in this case, viewable, by the BitTorrent user." (Footnote omitted).

Having reviewed the complaint, Plaintiff's motion, and the accompanying exhibits, I am satisfied that under these standards, there is good cause to issue the Rule 45 subpoena prior to the Rule 26(a) conference, in that there is no other reasonable alternative to discovering the Defendant's true identity.[3]

Accordingly, Plaintiff's motion for leave to serve third party subpoena [Doc. #2] is GRANTED, as follows:

1. Malibu may serve a Rule 45 subpoena on Internet Service Provider Comcast Cable, in order to identify the actual name and contact information for John Doe, who is associated with IP address 68.32.2.28. The subpoena will be limited to following information about John Doe: name, address, telephone number, and email address. A copy of this Opinion and Order shall be attached to any such subpoena.

2. Comcast shall in turn serve a copy of the subpoena and a copy of this order on the subscriber, defendant John Doe, within 30 days from the date of service of the subpoena on Comcast. Comcast may serve the subscriber 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. Nothing in this order precludes Comcast or Defendant John Doe from challenging the subpoena consistent with the Federal Rules of Civil Procedure and this court's Local Rules. However, any such challenge, such as a motion to quash the subpoena or a motion for a protective order, shall be filed before the return date of the subject subpoena, and the return date shall be no earlier than 30 days from the date of

---

[3] This case is distinguishable from others where Malibu Media names and seeks the identity of numerous John Doe defendants. *See, eg., Malibu Media, LLC v. Does 1-13*, 2012 WL 2800123 (E.D. Cal. 2012), where the court permitted a subpoena to only one of thirteen John Doe defendants.

service of the subpoena on Comcast.

4. If Comcast or the subscriber files a motion to quash or a motion for a protective order, Comcast shall preserve the information sought by the subpoena pending resolution of such a motion.

5. Any information disclosed to plaintiff by Comcast may only be used by Plaintiff for the purpose of protecting its rights under the Copyright Act, 17 U.S.C. §§ 101 et seq.[4]

IT IS SO ORDERED.

s/R. Steven Whalen
R. STEVEN WHALEN
UNITED STATES MAGISTRATE JUDGE

Dated: May 18, 2017

[4] There is nothing before me in this case to suggest that Malibu has ulterior or extrajudicial motives in seeking disclosure of the John Doe Defendant. However, numerous courts have remarked on what they have seen as chicanery in these cases. *See Malibu Media, LLC v. Does 1-13*, 2012 WL 2800123, *2, fn. 10 (E.D. Cal. 2012)(noting "some growing concern among district courts about these sorts of expedited discovery matters"). In *Malibu Media, LLC v. John Does 1-10*, 2012 WL 5382304 (C.D. Cal. 2012), the court remarked:

> "The federal courts are not cogs in a plaintiff's copyright-enforcement business model. The Court will not idly watch what is essentially an extortion scheme, for a case that plaintiff has no intention of bringing to trial. By requiring Malibu to file separate lawsuits for each of the Doe Defendants, Malibu will have to expend additional resources to obtain a nuisance-value settlement—making this type of litigation less profitable. If Malibu desires to vindicate its copyright rights, it must do it the old-fashioned way and earn it. "

See also Malibu Media, LLC v. Does 1–5, 2012 WL 2001968 at *1 (S.D.N.Y. 2012) (permitting limited discovery but stating that the court "shares the growing concern about unscrupulous tactics used by certain plaintiffs, particularly in the adult films industry, to shake down the owners of specific IP addresses from which copyrighted adult films were allegedly downloaded").

CERTIFICATE OF SERVICE

I hereby certify on May 18, 2017, that I electronically filed the foregoing paper with the Clerk of the Court sending notification of such filing to all counsel registered electronically. I hereby certify that a copy of this paper was mailed to non-registered ECF participants.

s/Carolyn Ciesla
Case Manager to
Magistrate Judge R. Steven Whalen