UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

MALIBU MEDIA, LLC,

Plaintiff,

v.

Case No. 15-10307
HON. AVERN COHN

JOHN DOE, subscriber assigned IP address 71.238.55.56,

Defendant.
_____/

ORDER DENYING DEFENDANT'S MOTION TO QUASH THIRD-PARTY SUBPOENA (Doc. 6)

I. INTRODUCTION

This is a copyright infringement case. Malibu Media, LLC (Plaintiff) is suing John Doe, subscriber assigned IP address 71.238.55.56 (Defendant). Plaintiff, the copyright owner to several adult motion pictures, claims that Defendant has violated the Copyright Act, 17 U.S.C. § 101, by illegally downloading and sharing the motion pictures, or a portion of the motion pictures, though an online file distribution network.

In January, the Court granted Plaintiff's Motion for Leave to Serve Third-Party Subpoena (Doc. 5). Now before the Court is Defendant's Motion to Quash Plaintiff's Third-Party Subpoena (Doc. 6). For the reasons that follow, Defendant's motion is DENIED.

II. BACKGROUND

At an unspecified date, Plaintiff, the owner of several adult motion pictures, hired

IPP International UG (IPP), to investigate copyright infringements over online file distributions networks.

Plaintiff says that Defendant used an online file distribution network called BitTorrent to illegally download, copy, and distribute Plaintiff's copyrighted motion pictures.[1] To identify Defendant as a potential infringer, IPP scanned the public

[1] BitTorrent is one of the most common file sharing systems for distributing large amounts of data. To distribute a large file, BitTorrent protocol breaks the file into many smaller pieces, which are exchanged between BitTorrent users and reassembled to complete the entire file. In *Third Degree Films v. Does 1–36*, No. 11–15200, 2012 WL 2522151 (E.D. Mich. May 29, 2012), under a similar set of facts to the present case, a court in this District described the function and process of BitTorrent 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 socalled "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

BitTorrent file distribution network for the presence of illegal transactions of Plaintiff's copyrighted motion pictures. IPP established a connection with Defendant's Internet Protocol (IP) address[2] and determined that Defendant had downloaded, copied, and distributed complete copies of Plaintiff's motion pictures without authorization. Although IPP had used Defendant's IP address to discover the identity and general location of the

---

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

Id. at *1–2 (citations and footnotes omitted).

[2] An IP address is a unique numerical label assigned to each device (e.g., computer, printer) participating in a computer network, which can be used to identify a particular location and device. IP addresses are assigned by a user's Internet Service Provider (ISP).

infringing device, it could not identify the name or address of the person involved in the infringement.

In January 2015, Plaintiff filed a Motion for Leave to Serve a Third-Party Supoena prior to a Rule 26(f) Conference. Specifically, Plaintiff sought to serve limited discovery on Defendant's Internet Service Provider (ISP) so that Plaintiff might learn Defendant's true identity. As noted above, the Court granted the motion.

III. STANDARD OF REVIEW

A motion to quash or modify a subpoena is governed by Fed. R. Civ. P. 45(d)(3). First, a court "must quash or modify a subpoena that: (i) fails to allow a reasonable time to comply; (ii) requires a person to comply beyond the geographical limits specified in Rule 45(c); (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or (iv) subjects a person to undue burden." Fed. R. Civ. P. 45(d)(3)(A). Further, a court "may, on motion, quash or modify the subpoena if it requires: (i) disclosing a trade secret or other confidential research, development, or commercial information; or (ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party." Fed. R. Civ. P. 45(d)(3)(B).

The party seeking to quash the subpoena bears the burden of demonstrating that the requirements of Rule 45 are satisfied. *Hendricks v. Total Quality Logistics, LLC*, 275 F.R.D. 251, 253 (S.D. Ohio 2011). Further, "a party does not have standing to quash a subpoena directed to a nonparty unless the party claims a privilege, proprietary interest, or personal interest in the information sought by the subpoena. The party

seeking to quash a subpoena bears a heavy burden of proof." *Lyons v. Leach*, 2014 WL 823411, at *1 (E.D. Mich. 2014) (citation omitted).

IV. DISCUSSION

A.

Defendant makes several arguments in support of the motion to quash. First, Defendant says that the Complaint provides no factual basis of copyright infringement by John Doe; "[t]herefore, it is reasonable to conclude that Plaintiff's Complaint and the third-party subpoena are intended solely to harass John Doe." (Doc. 6 at 5) Defendant says that even if there was a copyright infringement, the subpoena will identify the person who pays the Internet bill but not necessarily the proper defendant. Defendant says that Plaintiff's allegations are nothing more than "speculation that [Defendant's] IP's [sic] address was causing copyright infringement." (*Id.* at 7).

Next, Defendant argues that the object of the subpoena is to "cause undue burden by lowering [Defendant's] reputation in the community." (*Id.* at 6) Specifically, Defendant argues that by allowing Plaintiff to make public its allegations that Defendant "distributed material of questionable moral chastity," this would be damaging to Defendant's reputation and cause him extreme anguish and undue hardship. Plaintiff further says that any such public statement made by Plaintiff would be defamatory as libel per se under Michigan law.

Finally, Defendant argues that the subpoena should be quashed because Plaintiff violated Michigan privacy laws, M.C.L. 750.539d. This provision makes it illegal to "(a) [i]nstall, place, or use in any private place, without the consent of the person or

persons entitled to privacy in that place, any device for observing, recording, transmitting, photographing, or eavesdropping upon the sounds or events in that place;" or "(b) [d]istribute, disseminate, or transmit for access by any other person a recording, photograph, or visual image the person knows or has reason to know was obtained in violation of this section." M.C.L. 750.539d(a)-(b). Specifically, Defendant says that Plaintiff, without consent, "hacked into [Plaintiff's] computer and invaded into his privacy," and that "the investigator IPP retained by the Plaintiff accessed [Defendant's] computer and caused information . . . to be released." (Doc. 6 at 8).

B.

1.

Defendant's arguments are without merit. To begin, Plaintiff has proffered a sufficient factual basis to conclude that Defendant is the copyright infringer. The Complaint states that IPP established a connection with Defendant's IP address, and determined that a user at Defendant's IP address downloaded, copied, and distributed complete copies of Plaintiff's motion pictures without authorization. Other courts have explained that an infringing defendant's general denials of liability are not a sufficient basis for quashing a subpoena served on an ISP:

> A general denial of engaging in copyright infringement is not a basis for quashing the plaintiff's subpoena. It may be true that the putative defendants who filed motions and letters denying that they engaged in the alleged conduct did not illegally infringe the plaintiff's copyrighted movie, and the plaintiff may, based on its evaluation of their assertions, decide not to name these individuals as parties in this lawsuit. On the other hand, the plaintiff may decide to name them as defendants in order to have an opportunity to contest the merits and veracity of their defenses in this case. In other words, if these putative defendants are named as defendants in this case, they may deny allegations that they used BitTorrent to download and distribute illegally the plaintiff's movie, present

> evidence to corroborate that defense, and move to dismiss the claims against them. A general denial of liability, however, is not a basis for quashing the plaintiff's subpoenas and preventing the plaintiff from obtaining the putative defendants' identifying information.

Malibu Media LLC v. John Does 1-28, No. 12-CV-12598, 2012 WL 7748917, at *12-13 (E.D. Mich. Oct. 31, 2012) (citing *Voltage Pictures, LLC v. Does 1–5,000*, 818 F.Supp.2d 28, 35 (D.D.C.2011)). In addition, other courts have recognized that even if the subscriber is not the copyright infringer, the subscriber's identity is both relevant and discoverable. *TCYK, LLC v. Does 1–47*, No. 2:13–cv–539, 2013 WL 4805022, at *5 (S.D. Ohio Sept.9, 2013) ("[E]ven if discovery later reveals that a person other than the subscriber violated plaintiff's copyright, the subpoenaed information (the subscriber's contact information) is nevertheless reasonably calculated to lead to the discovery of admissible information, *i.e.*, the identity of the actual infringer.").

Here, there is sufficient factual basis to conclude that Defendant is the copyright infringer. Nor does any alleged lack of a factual basis lead to the conclusion that Plaintiff's Complaint and third-party subpoena were issued "solely to harass John Doe." (Doc. 6 at 5)

Finally, Defendant's objections do not fall into the limited category of rights or privileges that permit a party to seek to quash a subpoena issued to a nonparty. Here, Plaintiff had the subpoena served on the non-party ISP. There is no indication that the ISP has objected to the subpoena, appeared through counsel, or otherwise moved to quash the subpoena. Defendant does not claim a privilege, proprietary interest, or personal interest in the information sought by the subpoena. Here, Plaintiff seeks information related to Defendant's identity—information that Defendant has already

shared with his or her ISP. Such information does not provide a basis to quash the subpoena based on privilege or privacy interests. *See, e.g., Breaking Glass Pictures v. John Does 1–32*, No. 2:13–cv–849, 2014 WL 467137, at *4 (S.D. Ohio Feb. 5, 2014).

2.

The allegations in Plaintiff's Complaint are not defamatory under Michigan law. Under the litigation privilege, Plaintiff's allegations are immune from a defamation claim by Defendant. "Statements made during the course of judicial proceedings are absolutely privileged, provided they are relevant, material, or pertinent to the issue being tried. . . . The privilege should be liberally construed so that the participants in judicial proceedings are free to express themselves without fear of retaliation." *Sawyer v. Michigan State Police*, 310 F. Supp. 2d 876, 878 (E.D. Mich. 2004) (quoting *Maiden v. Rozwood*, 461 Mich. 109, 134 (1999)). Here, any such allegation related to copyright infringement of Plaintiff's motion pictures cannot be construed as defamatory.

In addition, to prevent any undue embarrassment to Defendant, Plaintiff does not object to allowing Defendant to remain anonymous and litigate this case as "John Doe." Any such embarrassment on the part of Defendant is not a sufficient reason to quash the subpoena.

3.

Finally, Defendant cannot establish a violation of Michigan's privacy laws. There is no evidence that Plaintiff or IPP "[i]nstall[ed], place[d], or use[d] . . . any device for observing, recording, transmitting, photographing, or eavesdropping upon the sounds or events in that place." Plaintiff or IPP did not "[d]istribute, disseminate, or transmit . . . a

recording, photograph, or visual image . . . obtained in violation of this section." M.C.L. 750.539d(a)-(b).

Here, Plaintiff's Complaint states that IPP used software to scan the *public* BitTorrent file distribution network, in order to isolate infringing transactions and the IP addresses used to download, copy, and distribute digital files containing Plaintiff's copyrighted motion pictures. Using the scanning protocol, IPP determined that a device located at Defendant's IP address was being used for an unlawful purpose. Neither Plaintiff nor IPP "hacked" into Plaintiff's computer. Rather, IPP joined the public BitTorrent file distribution network, recorded the IP addresses of infringers unlawfully sharing digital files containing Plaintiff's copyrighted motion pictures, and identified Defendant as one such user. IPP connected with Defendant's IP address, and downloaded from Defendant one or more pieces of the digital files. Defendant voluntarily shared the digital file pieces through the BitTorrent file distribution network. Defendant has no expectation of privacy in digital files transmitted over a public peer-to-peer file sharing network.

V. CONCLUSION

For the foregoing reasons, Defendant's motion to quash has been denied.

SO ORDERED.

s/Avern Cohn
UNITED STATES DISTRICT JUDGE

DATED: April 24, 2015

I hereby certify that a copy of the foregoing document was mailed to the attorneys of record on this date, April 24, 2015, by electronic and/or ordinary mail.

s/Sakne Chami
Case Manager, (313) 234-5160