UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

WELL GO USA, INC. A TEXAS CORPORATION,	§	
	§	
Plaintiff,	§	
v.	§	**CIVIL ACTION NO. 4:12-cv-00963**
	§	
UNKNOWN PARTICIPANTS IN FILESHARING SWARM IDENTIFIED BY HASH: B7FEC872874D0CC9B1372ECE5ED07AD7420A3BBB,	§	
	§	
Defendants.	§	

MEMORANDUM & ORDER

Before the Court is Plaintiff's Motion for Leave to Identify Defendants (Doc. No. 8) relating to the alleged copyright infringement of Plaintiff's movie, "Ip Man 2". Specifically, Plaintiff seeks the names of those it believes used BitTorrent technology to illegally share Ip Man 2. Based on Plaintiff's Motion and the applicable law, this court grants limited discovery.

I. BACKGROUND

BitTorrent is a peer-to-peer ("P2P") file sharing protocol used for distributing and sharing data on the Internet. Unlike other P2P protocols, BitTorrent downloading occurs through a piecemeal process by which a user can receive different portions of the file from multiple users. As soon as a user has downloaded a new piece of the file, she or he becomes able to transmit that piece to other peers. All peers who have a common BitTorrent file on their computer are considered a single "swarm." A swarm is identified by a unique hash tag, which Plaintiff identified in its complaint as "B7FEC872874D0CC9-

B1372ECE5ED07AD7420A3BBB." As long as users are connected to the BitTorrent protocol, they continue to distribute data to the peers in the swarm until the user manually disconnects from the swarm or the computer is shut down. *Diabolic Video Prods., Inc. v. Does 1–2099*, 2011 WL 3100404, *1–2 (N.D.Cal. May 31, 2011) cited by *K-Beech, Inc. v. John Does 1-41*, CIV.A. V-11-46, 2012 WL 773683 (S.D. Tex. Mar. 8, 2012).

Plaintiff attempts to join all Does who participated in the swarm from May 10, 2011 to July 15, 2011. (Compl. ¶ 12.) During this time, Plaintiff obtained each subscriber's IP address, the specific internet service provider (ISP), and the date and time of the infringing activity. (Doc. No. 8-3.) Plaintiff acknowledges that all Defendants did not engage with the swarm at the exact same time. (Doc. No. 8, at 7.)

Plaintiff requests leave of the court to identify each Defendant's name, address, telephone number, and email address. Plaintiff desires to use the subpoena provision of the Digital Millennium Copyright Act to compel ISPs to release Defendants' information. 17 USC § 512(h). In the alternative, Plaintiff requests permission to serve Rule 45 subpoenas on the ISPs. This Court grants limited discovery under Rule 45, subject to the protective order below.

II. ANALYSIS

A. Validity of Subpoena for Identifying Information

In order to seek a subpoena for identifying information of users, courts have weighed several factors to balance the need for disclosure against First Amendment interests. These factors include: (1) a concrete showing of a prima facie claim of actionable harm by the plaintiff; (2) specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) a central need for the subpoenaed

information to advance the claim; and (5) the user's expectation of privacy. *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 114 (2d Cir. 2010) citing *Sony Music Entm't Inc. v. Does 1-40*, 326 F.Supp.2d. 556, 565 (S.D.N.Y. 2004). *See also Call of the Wild Movie, LLC v. Does 1-1,062*, 770 F. Supp. 2d 332, 350 (D.D.C. 2011); *Interscope Records v. Does 1-14*, 558 F. Supp. 2d 1176, 1179 (D. Kan. 2008); *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 164 (D. Mass. 2008).

Plaintiff has asserted a prima facie claim for copyright infringement. Plaintiff's Complaint alleges that Plaintiff is the owner of Ip Man 2 and that Defendants downloaded Ip Man 2 without Plaintiff's authorization. Plaintiff claims that once this file was downloaded, it was a complete and accurate embodiment of Ip Man 2. Plaintiff has also provided the IP addresses of the individuals who were participating in the swarm and downloading the movie file illegally. (Doc. No. 8-3.) Plaintiff's complaint, along with the IP addresses, demonstrate a prima facie case (factor 1) and also demonstrate specificity (factor 2).

Plaintiff also must show that there is no alternate means to obtain the information (factor 3). Plaintiff states in its Motion that it has "obtained all information it possibly can without discovery from the service providers." Without expedited discovery to uncover Defendants' identifying information, the Court finds that Plaintiff cannot proceed. Plaintiff has also fulfilled factor 4, demonstrating a central need for the identifying information of Defendants. Plaintiffs cannot serve Defendants without knowing their identifying information, nor can Defendants respond to Plaintiff's allegations.

In terms of Defendants' expectation of privacy, under the protective order, Defendants will have a chance to object and respond to Plaintiff's claims, and will have a

chance to contest the subpoena before their names are turned over to Plaintiff. Thus, their information will remain private during the Court's determination of any motions that ISPs or Defendants wish to file (including a motion to quash, or to proceed anonymously). Thus, the Court believes that Defendants' First Amendment rights to anonymity do not prevent disclosure of identifying information.

B. Copyright Act Subpoena versus Rule 45 Discovery

Plaintiff seeks to identify Defendants under the Digital Millennium Copyright Act. 17 USC § 512(h). The first and most significant decision to interpret the extent of the subpoena authority of 512(h) was *Recording Industry Ass'n of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003). The *Verizon* court held that 512(h) authorized subpoenas only for ISPs that were actually storing infringing material, not simply acting as conduits for the material. In P2P protocols such as BitTorrent, ISPs do not generally store any infringing material. The material is located on users' computers (or in an off-line storage device, such as a compact disc), not on the ISP computers. *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc*., 351 F.3d 1229, 1235 (D.C. Cir. 2003).

Looking at both the language and the structure of the Act, the *Verizon* court rested its decision, in the main, on the text of 512(h) in relation to another subsection, 512(c)(3)(A). The court found that 512(h) required that subpoenas contain "a copy of a notification described in subsection [512](c)(3)(A)." *Verizon*, 351 F.3d at 1234. The notification provision of 512(c)(3)(A) "is found within one of the four safe harbors created by the statute to protect ISPs from liability for copyright infringement under certain

conditions." *In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 775 (8th Cir. 2005). Each safe harbor applies to a particular ISP function. The first safe harbor, under § 512(a), limits the liability of ISPs when they do nothing more than transmit, route, or provide connections for copyrighted material—that is, when the ISP is a mere conduit for the transmission. *Id.* Thus, a copyright owner cannot request a subpoena for an ISP which merely acts as a conduit for data.

Each of the other three safe harbors protects the ISP from liability if the ISP responds expeditiously to remove or disable access to infringing material. These three safe harbors require the ISP to be able both to locate and remove the infringing material, as a way of allowing the ISP to protect itself from liability. However, with P2P file sharing, the file itself is on the user's system and cannot be located or removed by the ISP.

Thus, the safe harbor implicated here, 512(a), limits the liability of an ISP when it merely acts as a conduit for infringing material. A number of other courts have read 512(h) in a similar manner. *In re Charter Communications,* 393 F.3d at 773; *In re Subpoena To Univ. of N. Carolina at Chapel Hill*, 367 F. Supp. 2d 945, 952 (M.D.N.C. 2005); *Interscope Records v. Does 1-7*, 494 F. Supp. 2d 388, 391 (E.D. Va. 2007). While this Court acknowledges it is not bound to follow the precedent of *Verizon,* it finds compelling the statutory analysis employed in *Verizon*.

Plaintiff lists nine ISPs in its Motion, but does not allege that all ISPs were storing infringing material on their servers (rather than merely acting as conduits). Plaintiff claims that Defendants using Verizon *may* have stored, shared, and viewed documents on Verizon's own servers. (Doc. No. 11.) However, there are eight other ISPs that were used by Doe Defendants. Because of the nature of P2P activity, these ISPs were likely used only

as conduits to download any infringing material. Thus, these ISPs likely fall within the safe harbor described in 512(a) and discovery should be granted through a different mechanism if possible.

Discovery can be granted under Rule 45 to obtain Defendants' identifying information, subject to a protective order. The protective order—issued under Rule 26(c)(1) of the Federal Rules of Civil Procedure—will allow the Doe Defendants and the ISPs to be heard before identifying information is released to Plaintiff. *See Hard Drive Productions, Inc. v. Does 1-59,* CIV.A. H-12-0699, 2012 WL 1096117 (S.D. Tex. Mar. 30, 2012); *Digital Sin, Inc. v. Does* 1-176, 279 F.R.D. 239, 242 (S.D.N.Y. 2012).

C. Joinder

The Court is also concerned as to whether Defendants are properly joined under Fed. R. Civ. P. 20(a). Courts are split on the question of whether a swarm of users can be joined in a single case. The Court recognizes that, while the Defendants participated in the same swarm in downloading Ip Man 2, this may not be considered the same transaction or occurrence, or the same series of transactions or occurrences. *Liberty Media Holdings, LLC v. BitTorrent Swarm*, 277 F.R.D. 669 (S.D. Fla. 2011); *CineTel Films, Inc. v. Does 1-1,052*, 853 F. Supp. 2d 545 (D. Md. 2012); *Patrick Collins, Inc. v. John Does 1–23*, 11–CV–15231, 2012 WL 1019034 (E.D.Mich. Mar. 26, 2012); *Hard Drive Prods., Inc. v. Does 1–30*, 2011 WL 4915551, at *4 (E.D.Va. Oct. 17, 2011); *Hard Drive Productions, Inc. v. Does 1-188*, 809 F. Supp. 2d 1150, 1156 (N.D. Cal. 2011). *But see Hard Drive Prods., Inc. v. Does 1–55,* 2011 WL 4889094, at *5 (N.D.Ill. Oct. 12, 2011) (finding joinder appropriate)*; Donkeyball Movie, LLC v. Does 1–171,* 810 F.Supp.2d 20, 26–27, 2011 WL 1807452, at *4 (D.D.C. May 12, 2011) (same).

In this case, the activity of all the Defendants occurred over a ten week period. One court, considering a lesser time span of swarm activity, found that, because the activity of the defendants occurred on "different days and times over a two-week period," there was "no evidence to suggest that each of the [defendants] 'acted in concert' with all of the others." *Hard Drive Productions, Inc. v. Does 1-188*, 809 F. Supp. 2d 1150, 1164 (N.D. Cal. 2011). There are also manageability difficulties and procedural inefficiencies to consider. *Hard Drive Productions, Inc. v. Does 1-130*, C-11-3826 DMR, 2011 WL 5573960 (N.D. Cal. Nov. 16, 2011). Joinder of the more than six hundred Defendants in this case could seriously delay litigation proceedings. *Liberty Media Holdings, LLC v. BitTorrent Swarm*, 277 F.R.D. 669, 672 (S.D. Fla. 2011). Defendants may also assert different factual and legal defenses. Permitting joinder would force the Court to address the unique defenses that are likely to be advanced by each individual Defendant, creating scores of mini-trials involving differening evidence and issues. *Hard Drive Prods., Inc.*, 809 F.Supp.2d at 1164.

On the other hand, Defendants were trading the exact same file as part of the same swarm. *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 244 (S.D.N.Y. 2012). One court considering joinder of Does over a three month period found that "each download of the file directly facilitated the others in such a way that the entire series of transactions would have been different but for each of Defendants' infringements." *Patrick Collins, Inc. v. Doe*, 2012 U.S. Dist. LEXIS 57187 (D. Md. Apr. 23, 2012).

The issue of joinder is better analyzed once unknown Defendants have been identified and served. *See MCGIP, LLC v. Does 1–18*, 2011 WL 2181620, at *1 (N.D.Cal. June 2, 2011); *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 244 (S.D.N.Y. 2012); *Hard*

Drive Productions, Inc. v. Does 1-59, CIV.A. H-12-0699, 2012 WL 1096117 (S.D. Tex. Mar. 30, 2012). After service, Defendants may present specific legal and factual defenses that would demonstrate the impropriety of permissive joinder. At this time, however, the Court finds that joinder is permissive for the purposes of carrying out the initial discovery and of gathering Defendants' identifying information in an efficient manner.

Finally, the Court notes that the relevant dates of the swarm listed on the Complaint (Compl. ¶12) are not the same as the dates that Plaintiff displayed in the Exhibits attached to its Motion. (Doc. No. 8-3.) Plaintiff alleges that the infringement started as early as April 8, 2011 and continued past July 10, 2011. However, the Court will allow discovery only for the IP addresses that were actually identified by Plaintiff's exhibit (Doc. No. 8-3). These IP addresses extend from Doe #1 on April 8, 2011 to Doe #643 on July 10, 2011.

III. PROTECTIVE ORDER

IT IS HEREBY ORDERED that Plaintiff may immediately serve Rule 45 subpoena on the ISPs listed in Doc. No. 8-1 to obtain information to identify Does 1–643, specifically her or his name, address, telephone number, and email address. The subpoena shall have a copy of this order attached.

IT IS FURTHER ORDERED that each ISP will have *60 days* from the date of service of the Rule 45 subpoena upon it to serve Does 1–643 with a copy of the subpoena and a copy of this order. Each ISP may serve Does 1–643 using any reasonable means, including written notice sent to her or his last known address, transmitted either by first-class mail or via overnight service.

IT IS FURTHER ORDERED that Does 1–643 shall have *60 days* from the date of service of the Rule 45 subpoena and this Order upon her or him to file any motions with

this Court contesting the subpoena (including a motion to quash or modify the subpoena), as well as any request to litigate the subpoena anonymously. The ISPs may not turn over the Doe Defendants' identifying information to Plaintiff before the expiration of this 60–day period and further order of the Court.

Additionally, if a Defendant or ISP files a motion to quash the subpoena, the Defendant or ISP should inform all ISPs so that the ISPs are on notice not to release any of the other Defendants' contact information until the Court rules on such motions.

IT IS FURTHER ORDERED that, if the 60–day period lapses without a Doe defendant or ISP contesting the subpoena, the respective ISPs will have 14 days to produce the subpoenaed information to Plaintiff.

IT IS FURTHER ORDERED that ISPs must take reasonable steps to preserve the subpoenaed information pending the resolution of any timely filed motion to quash. Any ISP may file a motion to address any undue burden caused by this preservation obligation.

IT IS FURTHER ORDERED that an ISP that receives a subpoena pursuant to this order shall confer with Plaintiff, and shall not assess any charge in advance of providing the information requested in the subpoena. An ISP that receives a subpoena and elects to charge for the costs of production shall provide a billing summary and cost report to Plaintiff.

IT IS FURTHER ORDERED that any information ultimately disclosed to Plaintiff in response to a Rule 45 subpoena may be used by Plaintiff only for the purpose of protecting its rights as asserted in its complaint. The information disclosed is limited to use by Plaintiff in this litigation and may not be disclosed other than to counsel for the parties.

IT IS SO ORDERED.

SIGNED in Houston, Texas, on this the 24th day of September, 2012.

KEITH P. ELLISON
UNITED STATES DISTRICT COURT JUDGE