

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

COBBLER NEVADA, LLC,)	
)	
Plaintiff,)	
)	No. 15 C 05277
v.)	
)	Judge John J. Tharp, Jr.
DOES 1-29,)	
)	
Defendants.)	

ORDER

This order supplements the Court’s prior order [10] granting Plaintiff’s motion for leave to take early discovery [7]. The motion is granted for the reasons stated below. However, Plaintiff may not publish the identities of the Doe defendants in any way without further leave of court. Additionally, within three business days after the information requested in the subpoena is produced, Plaintiff’s counsel is directed to provide the persons identified by that information with a copy of this order via overnight delivery. The Doe defendants so identified shall have 30 days from the date they receive a copy of the order to file an objection or other appropriate motion with this Court. The Doe defendants may proceed in this case by pseudonym (based on their Doe numbers or IP addresses) until further order.

STATEMENT

Plaintiff Cobbler Nevada, LLC brings a complaint for copyright infringement against twenty-nine unnamed “John Doe” defendants who, it alleges, unlawfully acquired and transferred the plaintiff’s copyrighted motion picture, “The Cobbler” (the “Movie”). The plaintiff alleges that it observed the defendants accessing the Movie using the BitTorrent protocol, but it has thus far been able to identify the defendants only by their Internet Protocol (“IP”) addresses and the dates and times when they accessed the Movie. The plaintiff now moves for leave to subpoena the non-party Internet Service Providers (the “ISPs”) from which the defendants obtained internet access in order to discover the defendants’ true identities.

Copyright infringement suits involving allegations of peer-to-peer file sharing using BitTorrent are now familiar to district courts. BitTorrent is a software protocol that facilitates the practice of peer-to-peer file sharing used to distribute large amounts of data over the internet. To share information using BitTorrent, an initial file-provider (the “seeder”) elects to share an initial file, called a “seed,” with a torrent network. The file to be distributed is divided into segments called “pieces.” Other users (“peers”) intentionally connect to the seed file to download it. As each peer receives a new piece of the file, the peer also immediately becomes a source of that piece for other peers, relieving the original seeder from having to send that piece to every peer requesting a copy. This is the key difference between BitTorrent and earlier peer-to-peer file sharing systems: “BitTorrent makes file sharing a cooperative endeavor.” Sean B. Karunaratne,

Note, *The Case Against Combating BitTorrent Piracy Through Mass John Doe Copyright Infringement Lawsuits*, 111 Mich. L. Rev. 283, 290 (2012) [hereinafter, *The Case Against Mass Joinder*]. It is “architecturally impossible for any peer on the network to take without giving.” *Id.* at 288.

After a peer completely downloads the file, it continues to transmit pieces of the file to other users until it disconnects from BitTorrent. As additional peers request and receive pieces of the same file, each user becomes a part of the network from which the file can be downloaded. As more users join the network, the speed and efficiency of downloads increases. The group of seeders and peers uploading and downloading the identical file are called a “swarm.” While connected to the swarm, users continuously download pieces of the file until they have obtained a complete file and continuously upload pieces of the file to other users in the swarm. Even after a user exits the swarm, the identical file pieces that the user downloaded from other users and then shared with peers continue to circulate throughout the swarm. BitTorrent swarms can survive continuously for months, beyond the point at which an individual user exits the swarm.

The plaintiff alleges that the defendants each joined the same BitTorrent swarm to download and upload the Movie. The plaintiff retained Maverickeye (the “Investigator”) to identify the IP addresses of those BitTorrent users who were copying and distributing the Movie. The Investigator used forensic software to scan peer-to-peer networks for the presence of potentially infringing transactions, isolating the transactions and IP addresses of BitTorrent users who copied and distributed the Movie as part of the same swarm. The Investigator confirmed that each of the defendants was in the same swarm because each downloaded file was identified by the same “hash checksum.” A hash checksum is a string of alphanumeric characters generated by applying a mathematical algorithm to a digital file; any differences in the digital file will cause the algorithm to produce a different result. The Investigator also used geolocation functionality to confirm the location of each of the IP addresses it identified. Although IP addresses do not reveal the names or contact information of the subscribers, they do reveal the location of the IP address used for the transaction; the IP addresses here are located in cities and towns within this district. The Investigator reported that each defendant participated in the swarm by downloading the Movie from a single seed file between March 13, 2015, and March 14, 2015. Finally, the Investigator confirmed that the files downloaded from the defendants, when reassembled using a BitTorrent client, result in a fully playable motion picture.

The plaintiff seeks leave to subpoena the ISPs associated with the IP addresses it has identified as belonging to users who participated in the swarm. The plaintiff will ask the ISPs to provide information sufficient to identify each defendant by name and current mailing address. If the ISPs cannot themselves identify one or more of the Doe defendants but can identify an intermediary ISP as the entity providing online services and/or network access to such Doe defendants, the plaintiff will then serve a subpoena on that ISP requesting the identifying information for the relevant Doe defendants.

Fed. R. Civ. P. 26(d) prohibits parties from seeking discovery “from any source” before the parties have conferred in accordance with Rule 26(f), except when authorized by the Federal Rules of Civil Procedure, stipulation, or a court order. District courts have broad discretion in managing the discovery process. *See James v. Hyatt Regency Chi.*, 707 F.3d 775, 784 (7th Cir. 2013). Courts “evaluate a motion for expedited discovery ‘on the entirety of the record to date

and the reasonableness of the request in light of all the surrounding circumstances.” *Ibarra v. City of Chi.*, 816 F. Supp. 2d 541, 554 (N.D. Ill. 2011) (quoting *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. O’Connor*, 194 F.R.D. 618, 624 (N.D. Ill. 2000)). Under the circumstances here, it is reasonable to allow the plaintiff the opportunity to discover the defendants’ true identities prior to any Rule 26(f) conference. The plaintiff seeks to discover only the names and current mailing addresses of the defendants. The plaintiff needs this expedited discovery because it will otherwise be unable to maintain this litigation, as it has no other way of identifying the defendants. And the defendants will not be burdened by the plaintiff’s requests, as their ISPs, rather than the defendants themselves, will be required to respond to the subpoenas.

One issue that bears further discussion is the plaintiff’s joinder of multiple Doe defendants in a single civil complaint. A plaintiff may join defendants in a suit presenting any question or law or fact common to all defendants if “any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences.” Fed. R. Civ. P. 20(a)(2)(A). There is a split of authority nationally and within this district over whether it is appropriate to join in a single lawsuit many anonymous defendants who are alleged to have participated in a single BitTorrent swarm. Compare, e.g., *Site B, LLC v. Does 1-51*, No. 13 C 5295, 2014 WL 902688, at *2-4 (N.D. Ill. Mar. 7, 2014) (allowing joinder); *TCYK, LLC v. Does 1-44*, No. 13-cv-3825, 2014 WL 656786, at *3 (N.D. Ill. Feb. 20, 2014) (same); *Malibu Media, LLC v. Does 1-6*, 291 F.R.D 191, 202 (N.D. Ill. 2013) (same); *Pacific Century Int’l v. Does 1-31*, No. 11 C 9064, 2012 WL 2129003, at *3 (N.D. Ill. June 12, 2012) (same); *First Time Videos, LLC v. Does 1-76*, 276 F.R.D. 254, 257 (N.D. Ill. 2011) (same); *Digital Sin, Inc. v. Does 1-27*, No. 12 Civ. 3873(JMF), 2012 WL 2036035, at *2 (S.D.N.Y. June 6, 2012) (same); with, e.g., *Dall. Buyers Club, LLC v. Does 1-28*, No. 14 C 4927, 2014 WL 3642163, at *1 (N.D. Ill. July 22, 2014); *reFX Audio Software Inc. v. Does 1-85*, No. 13 C 01790, 2014 WL 1293816, at *6 (N.D. Ill. Mar. 24, 2014) (same); *Malibu Media, LLC v. Reynolds*, No. 12 C 6672, 2013 WL 870618, at *14 (N.D. Ill. Mar. 7, 2013) (same); *Digital Sins, Inc. v. Does 1-245*, No. 11 Civ. 8170(CM), 2012 WL 1744838, at *2 (S.D.N.Y. May 15, 2012) (same).

The disagreement among the courts centers on the question of whether claims against multiple defendants who participated in the same BitTorrent swarm arise out of the same transaction or series of transactions, as required for joinder under Rule 20(a)(2)(A). The D.C. Circuit—the only federal appellate court to have addressed this question in the BitTorrent context—recently sided with those district courts that reject joinder, concluding that “the mere fact that two defendants accessed the same file through BitTorrent provides an insufficient basis for joinder.” *AF Holdings, LLC v. Does, 1-1058*, 752 F.3d 990, 998 (D.C. Cir. 2014). In reaching this finding, the D.C. Circuit emphasized that the case before it involved 1,058 Does and “a period of nearly *five months*,” and that the plaintiff had “provided no reason to think that the Doe defendants . . . were ever participating in the same swarm at the same time.” *Id.*

As Judge Dow has pointed out, the Federal Circuit also recently addressed the meaning of “series of transactions or occurrences,” albeit not within the context of a BitTorrent case. See *TCYK*, 2014 WL 656786, at *3 (citing *In re EMC Corp.*, 677 F.3d 1351, 1358 (Fed. Cir. 2012)). The Federal Circuit noted that “the mere fact that a case involves independent actors as defendants does not necessarily bring the case outside the scope of Rule 20.” *In re EMC Corp.*, 677 F.3d at 1357. Citing both the Wright and Miller treatise and Supreme Court case law, the

court concluded that such defendants “satisfy the transaction-or-occurrence test of Rule 20 when there is a logical relationship between the separate causes of action,” which “enables the federal courts to promote judicial economy by permitting all reasonably related claims for relief by or against different parties to be tried in a single proceeding under the provisions of Rule 20.” *Id.* at 1358 (quoting 7 Charles Alan Wright et al., *Federal Practice and Procedure* § 1653 (3d ed. 2001)).

Though there are strong arguments on both sides of this issue, entering a *sua sponte* finding of misjoinder of the Doe defendants would, in the Court’s judgment, be inappropriate at this early stage. The plaintiff alleges that each defendant deliberately participated in a BitTorrent swarm that consisted of a series of transactions in which swarm participants shared pieces of the same file with one another over a period of a single day. When the defendants allegedly joined the swarm, they consented (implicitly, at least) both to download pieces of the Movie from other members of the swarm *and* to upload pieces of the Movie to other swarm participants. For at least the period that the defendants were connected to the swarm, a logical relationship exists between the defendants’ conduct. Even critics of mass joinder in copyright infringement cases concede that joinder of defendants who participate contemporaneously in a swarm is appropriate. *See, e.g., The Case Against Mass Joinder, supra*, at 293.

Of course, some of the defendants in this case were part of the alleged swarm at different times. If Doe 1 left the swarm before Doe 10 joined, then Doe 1 could not, of course, have provided a piece of the file to Doe 10 directly. That fact suggests to some that joinder of Does 1 and 10 would not be appropriate. *See, e.g., AF Holdings*, 752 F.3d at 998 (assuming for purposes of the case that “individuals who participate in the same swarm *at the same time* are part of the same series of transactions within the meaning of Rule 20(a)(2)”; *Reynolds*, 2013 WL 870618, at *13 (stating that joinder is appropriate where defendants accessed the swarm simultaneously or within hours of one another); *Digital Sins, Inc. v. Does 1-245*, 2012 WL 1744838, at *2 (rejecting joinder where defendants shared movie “in separate and isolated incidents over the course of 59 days”); *The Case Against Mass Joinder, supra*, at 294-95. That argument, however, appears to overlook the fact that the pieces of the file that Doe 1 distributed directly to other Does who were in the swarm contemporaneously with Doe 1 were in turn subsequently distributed by them to the Does who joined the swarm after Doe 1 left it; in the context of a swarm, there is only a single digital file that is distributed among the members. Thus, it cannot be said that subsequent transfers of that file are even entirely “independent” of the earlier transfers; all of the transfers involve the same file and the earlier transfers of the pieces of that file facilitate the later transfers. Moreover, nothing in Rule 20 suggests that joinder requires a direct transaction between every defendant. To the contrary, the language of the rule permitting joinder where there has been a “series” of transactions seems expressly to contemplate that the transactional link between parties may be more attenuated. These considerations have prompted a number of courts to conclude that joinder in these cases may extend more broadly than contemporaneous participation in a swarm would allow. *See, e.g., TCYK*, 2014 WL 656786, at *3 (holding that a logical relationship exists among the actions of the defendants “[r]egardless of whether [they] contemporaneously participated in the swarm”); *Third Degree Films v. Does 1-47*, 286 F.R.D. 188, 195 n.11 (D. Mass. 2012) (“[T]he Court holds that the interaction of the Doe defendants via BitTorrent—even if indirect—is significant enough to bring them within the broad scope of permissibly joined parties under Rule 20(a.)”); *Third Degree Films v. Does 1-36*, No. 11-cv-15200, 2012 WL 2522151, *9 (E.D. Mich. May 29, 2012) (“Therefore, Doe No. 10

plausibly *indirectly* uploaded pieces of the work to, say, Doe No. 25 who participated in the swarm four days later.”); *cf. Lozada v. City of Chi.*, No. 10 C 1019, 2010 WL 3487952, at *2 (N.D. Ill. Aug. 30, 2010) (“Although ‘transaction or occurrence’ is not defined in Rule 20(a), courts interpret this term as ‘comprehend[ing] a series of many occurrences, depending not so much upon the immediateness of their connection as upon their logical relationship.’” (quoting *Mosley v. Gen. Motors Corp.*, 497 F.2d 1330, 1333 (8th Cir. 1974))).

As noted above, BitTorrent requires a cooperative endeavor among those who use the protocol. Every member of a swarm joins that endeavor knowing that, in addition to downloading the file, they will also facilitate the distribution of that identical file to all other members of the swarm, without regard to whether those other members were in the swarm contemporaneously or whether they joined it later. In that light, permitting joinder among non-contemporaneous swarm participants does not seem novel or extreme; the law governing joint ventures and conspiracies, for example, permits plaintiffs to proceed against groups of defendants who engaged in a cooperative endeavor to facilitate an unlawful object whether or not all of the members of the group took part in all of the actions of the group and without regard to when the members joined the group. *See, e.g., State of Ohio ex rel. Fisher v. Louis Trauth Dairy*, 856 F. Supp. 1229, 1239-40 (S.D. Ohio 1994) (allowing joinder of all defendants who allegedly participated in any of three overlapping conspiracies to violate the antitrust laws); *Krehl v. Baskin-Robbins Ice Cream Co.*, 78 F.R.D. 108, 116 (C.D. Cal. 1978) (where conspiracy defendants share a common objective, it makes no difference that they join the “conspiracy at different times and at different places, or that they [do] not personally know one another or all details of the conspiracy everywhere”).

That is not to say that it would necessarily be appropriate to join every participant in a long-running swarm that persisted indefinitely. These are analogies, and may break down at the extremes, but for purposes of this issue, in this case, they suggest that it would be premature to deny the plaintiff an opportunity to identify by name the potential defendants in this suit. Here the plaintiff has limited its complaint to participants who are likely located in this district and who participated in a swarm over a brief time frame of slightly more than 24 hours.¹ The Court will not *sua sponte* find misjoinder at this time and will grant the plaintiff leave to issue the subpoenas it proposes. The Court recognizes, however, that no defendant has had the opportunity to brief the joinder issue, and this ruling does not foreclose any future challenge to the propriety of joinder in this case. The Doe defendants may raise the issue if they so choose.

Though the plaintiff may issue subpoenas to determine the defendants’ true identities, the plaintiff is prohibited from naming the Doe defendants in an amended complaint or otherwise publishing their identities in any way without leave. BitTorrent litigation often involves “matters of a sensitive and highly personal nature,” *Sunlust Pictures, LLC v. Does 1-75*, No. 12 C 1546,

¹ Further, while many BitTorrent cases arise in the context of pornographic movies, others, including this case, do not. Thus, none of the concerns that animate many of the opinions rejecting joinder in BitTorrent cases involving pornographic films—such as the potential for unfair, if not extortionate, settlement practices—are present here. In any event, courts should be hesitant to fashion rules that may be based more on distaste for the copyrighted works or the nature of a plaintiff’s business rather than on application of neutral legal principles.

2012 WL 3717768, at *5 (N.D. Ill. Aug. 27, 2012) (citing *Southern Methodist Univ. Ass'n of Women Law Students v. Wynne & Jaffe*, 599 F.2d 707, 712-13 (5th Cir. 1979)), and even where—as here—that is not a factor, there remains a substantial possibility that the names turned over by ISPs will not accurately identify the individuals who actually downloaded or shared the copyrighted material, *see, e.g., Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 242 (S.D.N.Y. 2012) (noting that the plaintiff there estimated that 30 percent of the individuals whose names were disclosed to plaintiffs did not download the copyrighted material). Balancing these concerns against the public's interest in knowing the defendants' true identities, the Court finds that allowing the defendants to proceed by pseudonym is appropriate at this preliminary stage of the litigation, when no defendant has been put on notice of this suit. Once the defendants have received such notice, the Court will revisit the issue of whether the names of the defendants in this matter may be publicly disclosed.



John J. Tharp, Jr.
United States District Judge

Date: July 16, 2015