

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X		:	
MALIBU MEDIA, LLC,		:	
	Plaintiff,	:	12 Civ. 2955 (PAE)
		:	
	-v-	:	<u>OPINION &amp; ORDER</u>
		:	
JOHN DOES 1-4,		:	
	Defendants.	:	
-----X		:	

PAUL A. ENGELMAYER, District Judge:

Plaintiff Malibu Media, LLC filed an *ex parte* motion seeking permission to take discovery, before a Rule 26(f) conference, from third-party Internet Service Providers (“ISPs”) to identify the names, addresses, telephone numbers, email addresses, and Media Access Control (“MAC”) addresses associated with identified Internet Protocol (“IP”) addresses that Malibu Media alleges were used to illegally share a file containing its copyrighted motion picture in violation of 17 U.S.C. § 101 *et seq.* For the reasons that follow, the motion to serve Rule 45 subpoenas on third-party ISPs is granted in part, pursuant to a protective order, and denied in part.

**I. BACKGROUND<sup>1</sup>**

Malibu Media is a California corporation that produced a motion picture entitled “Tiffany Teenagers in Love” (the “movie”). Malibu Media registered a copyright for the movie in

---

<sup>1</sup> The facts which form the basis of this Opinion are taken from the Complaint, with exhibits, and the Declaration of Tobias Fieser in support of the motion for expedited discovery, with exhibits. Unless otherwise noted, no further citation to sources will be made. For the purposes of this Opinion only, the Court takes all facts as pleaded in the Complaint, and in the motion for expedited discovery, as true.

November 2011. John Does 1-4 (“Does 1-4” or the “Doe defendants”) are 4 unknown individuals associated with the 4 IP addresses named in the Complaint.

Malibu Media’s Complaint arises from the illegal distribution of copies of the movie through peer-to-peer file-sharing networks. Peer-to-peer file-sharing networks facilitate the sharing of very large files among individual computer users. In this instance, one copy of the movie (distinguishable from other copies by a unique piece of forensic data known as a “hash”) was shared by and downloaded by multiple Internet users in what is referred to as a “swarm.” A swarm is a group of Internet users who come together to download and then, in turn, distribute by sharing with others, a file.

Malibu Media did not consent to the distribution of unlawful copies of the movie, a copyrighted work, by way of swarms. The subject of this lawsuit is an unlawful copy of the movie that was shared by a swarm believed by Malibu Media—and confirmed by reverse-IP looks-ups—to consist of Internet users in the greater New York City area, in New York State,<sup>2</sup> during the months of December 2011 and January and February 2012. Malibu Media does not know the actual identity of the individuals who participated in the swarm; the primary identification information they have are these individuals’ IP addresses. ISPs assign IP addresses to subscribers, and, generally, keep records that correlate a subscriber’s true identity (*e.g.*, name, address, and email address) to that subscriber’s IP address.

---

<sup>2</sup> In the Complaint, Malibu Media alleges that personal jurisdiction in New York State and venue in the Southern District are proper because, after undertaking efforts to geographically pinpoint Does 1-4, it believes they are all located in New York State, in and around New York City. Malibu Media incorporates into its Complaint a listing of the believed cities and states of residence of Does 1-4, and each is believed, based on research, to reside in New York. For the limited purposes of this Opinion only, those research-based allegations as to the propriety of jurisdiction and venue suffice. *See Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 241 n.3 (S.D.N.Y. 2012) (“*Digital Sin I*”).

On April 13, 2012, Malibu Media filed its Complaint in this action (Dkt. 1). On April 25, 2012, it filed this motion to take discovery before a Rule 26(f) conference (Dkt. 4). Malibu Media seeks to obtain from the third-party ISPs, by way of a Rule 45 subpoena, the names, addresses, telephone numbers, email addresses, and MAC addresses associated with the IP addresses that participated in the swarm.

## **II. DISCUSSION**

### **A. Joinder of Does 1-4**

Under Federal Rule of Civil Procedure 20(a)(2), persons “may be joined in one action as defendants if . . . any right to relief is asserted against them . . . with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences” and “any question of law or fact common to all defendants will arise in the action.” “Under the Federal Rules of Civil Procedure, ‘the impulse is toward entertaining the broadest possible scope of action consistent with fairness to the parties; joinder of claims, parties and remedies is strongly encouraged.’” *Digital Sin I*, 279 F.R.D. at 243 (quoting *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 724 (1966)). Here, Malibu Media argues that Does 1-4 have been properly joined, because they traded, through cooperative uploading and downloading, the same file of the movie in a swarm.

In recent months, courts in this district and around the country have considered the propriety of joinder in similar copyright cases, all naming multiple John Doe defendants. Some courts that have considered this issue have found joinder improper, whereas others have found for joinder in cases similarly postured to this one. *See, e.g., Digital Sin I*, 279 F.R.D. at 243 nn.4-5 (collecting cases). This Court is persuaded by the standard articulated by the Hon. Paul A. Crotty, in *DigiProtect USA Corp v. Does 1-240*, No. 10-cv-8790, 2011 WL 4444666 (S.D.N.Y. Sept. 26, 2011) and the Hon. Alison J. Nathan, in *Digital Sin, Inc.*: At this initial

stage, joinder is proper if plaintiff specifically alleges defendants' connection to the same swarm. *See Digital Sin I*, 279 F.R.D. at 244; *DigiProtect USA Corp.*, 2011 WL 4444666, at \*3 n.3. Here, Malibu Media makes such concrete allegations, based on research which indicates these transactions involved one file, marked by the same hash, traded among geographically centralized individuals over a three-month period. Accordingly, joinder of the Doe defendants is, at this stage of the case, appropriate.

**B. Pre-Conference Discovery**

Generally, Federal Rule of Civil Procedure 26 calls for the parties to meet and confer prior to commencing discovery, but provides for earlier discovery pursuant to a court order. *See* Fed. R. Civ. P. 26(d), (f). Courts in this district "have applied a 'flexible standard of reasonableness and good cause' to determine whether expedited discovery is appropriate." *Digital Sin Inc. v. Does 1-27*, No. 12-cv-3873, 2012 WL 2036035, at \*3 (S.D.N.Y. June 6, 2012) ("*Digital Sin IP*") (quoting *Ayyash v. Bank Al-Madina*, 233 F.R.D. 325, 326-27 (S.D.N.Y. 2005)). This Court follows the recent precedents set by other courts in this district in nearly identical circumstances in finding that such good cause exists here for granting Malibu Media's motion to the extent it seeks expedited discovery of the names, addresses, email addresses, and MAC addresses *only* of Does 1-4. *See, e.g., Digital Sin II*, 2012 WL 2036035, at \*4; *Digital Sin I*, 279 F.R.D. at 241. As in those cases, plaintiff has no reasonable means other than through the ISPs by which to identify the individuals allegedly involved in the swarm, and the ISPs, in turn, are statutorily prohibited from providing this information to Malibu Media absent a court order. *See* 47 U.S.C. § 551(c); *Digital Sin I*, 279 F.R.D. at 241. Accordingly, Malibu Media may seek expedited discovery of the names, addresses, email addresses, and MAC addresses of Does 1-4, pursuant to a protective order, as discussed below.

The Court denies Malibu Media's motion for pre-conference discovery to the extent it seeks the telephone numbers of Does 1-4. This information is at best duplicative, in that Malibu Media is already seeking the Doe defendants' physical addresses and email addresses, and at worst, it opens up the Doe defendants to potential harassment.

**C. Protective Order**

Pursuant to Federal Rule of Civil Procedure 26(c), a "court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." As other district courts encountering similar cases have noted, the high risk of "false positives" in the identification process (*e.g.*, one person's name and other identifying information is associated with the ISP account, but the copyrighted material was downloaded and uploaded by a different individual), combined with the sensitive nature of the copyrighted material at issue, may lead to a certain amount of undue annoyance and embarrassment for a non-culpable party. *See, e.g., Digital Sin II*, 2012 WL 2036035, at \*4. Accordingly, the Court finds good cause for the issuance of a protective order, as outlined below.

## CONCLUSION

For the reasons given above, it is hereby ORDERED that:

(1) Malibu Media may immediately serve a Rule 45 subpoena on the ISPs listed in Exhibit A to the Complaint to obtain the names, addresses, email addresses, and MAC addresses *only* of Does 1-4. The subpoena shall have a copy of this Order attached;

(2) The ISPs shall have 30 days from the date of service of the Rule 45 subpoena and this Order upon them to serve Does 1-4 with a copy of the subpoena and a copy of this Order. The ISPs may serve Does 1-4 using any reasonable means, including written notice to a last known address, transmitted either by first-class mail or via overnight service;

(3) Does 1-4 shall have 30 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, as well as any requests to litigate the subpoena anonymously. The ISPs may *not* turn over the Doe defendants' information to Malibu Media prior to the close of this 30-day period. Additionally, if a defendant or an ISP files a motion to quash the subpoena, the ISPs may not turn over any information to Malibu Media until the issues have been addressed and the Court issues an Order instructing the ISPs to resume in turning over the requested discovery;

(4) If that 30-day period closes without a Doe defendant or an ISP contesting the subpoena, the ISPs shall then have 10 days to produce the information responsive to the subpoena to Malibu Media. A Doe defendant or ISP who moves to quash or modify the subpoena, or to proceed anonymously, shall, at the same time as her or his filing, also notify all ISPs so that the ISPs are on notice not to release any of the Doe defendants' information to Malibu Media until the Court rules on any such motions;

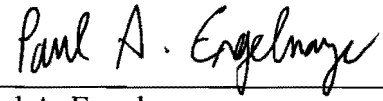
(5) The ISPs shall preserve any subpoenaed information pending the resolution of any timely-filed motion to quash;

(6) An ISP that receives a subpoena pursuant to this order shall confer with Malibu Media 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 Malibu Media;

and

(7) Any information ultimately disclosed to Malibu Media in response to a Rule 45 subpoena may be used by Malibu Media solely for the purpose of protecting its rights as set forth in its Complaint.

SO ORDERED.



---

Paul A. Engelmayer  
United States District Judge

Dated: July 31, 2012  
New York, New York