UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

NEW SENSATIONS, INC.,		
Plaintiff,	:	12 Civ. 3534 (PAE)
-v-	:	OPINION & ORDER
JOHN DOES 1-32,		
Defendants.		

PAUL A. ENGELMAYER, District Judge:

Plaintiff New Sensations, Inc. 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, email addresses, and Media Access Control ("MAC") addresses associated with identified Internet Protocol ("IP") addresses that New Sensations 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, pursuant to a protective order.

I. BACKGROUND[1]

New Sensations is a California corporation that produced a motion picture entitled "Seinfeld #2: A XXX Parody" (the "movie"). The movie is copyrighted and is available for

[1] The facts which form the basis of this Opinion are taken from the Complaint, with exhibits, and the Declaration of Jon Nicolini 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.

purchase. John Does 1-32 ("Does 1-32" or the "Doe defendants") are 32 unknown individuals associated with the 32 IP addresses named in the Complaint.

New Sensations'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.

New Sensations 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 New Sensations—and confirmed by reverse-IP looks-ups—to consist of Internet users in and around New York City, in New York State,[2] during the months of January, February, and March 2012. New Sensations 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.

[2] In the Complaint, New Sensations alleges that personal jurisdiction in New York State and venue in the Southern District are proper because, after undertaking efforts to geographically pinpoint Does 1-32, it believes they are all located in New York State, in and around New York City, and because "each Defendant contracted with an [ISP] found in this District." New Sensations incorporates into its Complaint a listing of the believed state of residence of Does 1-32, 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 May 3, 2012, New Sensations filed its Complaint in this action (Dkt. 1). On May 8, 2012, it filed this motion to take discovery before a Rule 26(f) conference (Dkt. 2). New Sensations seeks to obtain from the third-party ISPs, by way of a Rule 45 subpoena, the names, addresses, email addresses, and MAC addresses associated with the IP addresses that participated in the swarm.

II. DISCUSSION

A. Joinder of Does 1-32

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, New Sensations argues that Does 1-32 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 proprietary 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 case 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, New Sensations 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 II*") (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 New Sensations's motion for expedited discovery. *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 New Sensations absent a court order. *See* 47 U.S.C. § 551(c); *Digital Sin I*, 279 F.R.D. at 241. Accordingly, New Sensations may conduct expedited pre-conference discovery, pursuant to a protective order, as discussed below.

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 an 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.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.