

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

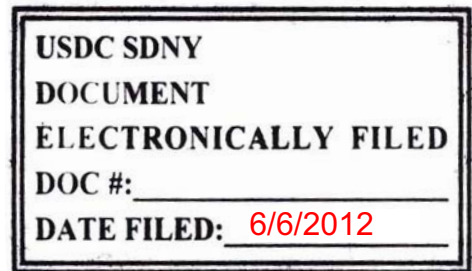
-----X  
DIGITAL SIN, INC.,

Plaintiff,

-v-

DOES 1-27,

Defendants.  
-----X



12 Civ. 3873 (JMF)

OPINION AND ORDER  
PERMITTING LIMITED  
EXPEDITED DISCOVERY  
PURSUANT TO A  
PROTECTIVE ORDER

JESSE M. FURMAN, District Judge:

Plaintiff Digital Sin, Inc. (“Digital Sin”) brings this action, alleging copyright and contributory infringement, against 27 defendants whose identities are unknown to Digital Sin at this time. (Compl. ¶¶ 1-2 (Docket No. 1)). For now, Digital Sin identifies each defendant solely by the Internet Protocol (“IP”) address assigned to the defendant by his or her Internet Service Provider (“ISP”). (Compl. ¶ 7, Ex. A). On the same day it filed the complaint, plaintiff filed an *ex parte* motion for expedited discovery — namely, for leave to serve subpoenas pursuant to Rule 45 of the Federal Rules of Civil Procedure on various ISPs for information sufficient to identify each defendant, including name, current and permanent address, e-mail address, and Media Access Control address. (Pl.’s Mot. (Docket No. 3)). For the reasons stated below, the motion for leave to take expedited discovery is GRANTED, but subject to a protective order.

**BACKGROUND**

The following background is drawn from plaintiff’s complaint and materials submitted in support of its motion, and is accepted as true for purposes of this motion. Digital Sin, a California corporation, produced a motion picture (the “Video”) and released it on digital video disc through various vendors, including www.cduniverse.com, in January 2012. (Compl. ¶ 8).

In its complaint, Digital Sin identifies the Video only by copyright registration number, but plaintiff's business is the production and distribution of pornographic movies and other cases brought by plaintiff, some of which are discussed below, have involved pornographic movies, so it seems safe to assume that the Video is a pornographic movie. (Compl. ¶ 8). Plaintiff alleges that defendants copied the Video using torrent software — the most common of which is BitTorrent — which enables users to share files online. (Compl. ¶ 5).

To the extent relevant here, BitTorrent enables users to download an electronic file in small pieces or blocks from multiple other users. (Nicolini Decl. ¶¶ 10-15; *Id.* Ex. I (Docket No. 5)). Each content file is divided into those blocks by an associated “torrent” file, which is identified by a unique hash number — an alphanumeric sequence corresponding only to that torrent file. (*Id.* ¶ 9; Compl. ¶ 11). Thus, even if two separate torrent files were created to share the same copyrighted work, the torrents would have separate hash numbers. (Nicolini Decl. ¶ 25). While downloading the file from other users, the user simultaneously uploads to other BitTorrent users the portions of the file he or she has already downloaded. (*Id.* ¶ 11; Compl. ¶ 9). The group of interacting users who share the same file is known colloquially as a “swarm.” (Nicolini Decl. ¶ 11). The users who constitute a “swarm” must expose their own IP addresses to one another as part of the sharing process. (*Id.* ¶ 26; Compl. ¶ 12).

A BitTorrent user's decision to join a “swarm” by downloading the torrent file and participating in the sharing of the file is, according to a declaration submitted by plaintiff in support of its motion, a “deliberate act.” (Nicolini Decl. ¶ 16.) The user derives a benefit from the interconnected architecture of the BitTorrent protocol — namely the increased speed, efficiency, and reliability of his or her downloading activity. (*Id.* Ex. I (“The more popular a large video, audio or software file, the faster and cheaper it can be transferred with

BitTorrent.”)). This benefit is heightened as more and more users participate in a single “swarm.” (*Id.*). Thus, even though a user may not know the identities of the others with whom he or she is cooperating, and cannot choose with whom he or she connects to upload and download the file at issue, the user is continuously connecting to other members of the “swarm,” and thus benefits from the joint sharing activities of the other participants in the “swarm.”

In the present case, Digital Sin alleges that the 27 Doe defendants traded (that is, simultaneously downloaded and uploaded) the Video as part of a single “swarm” and within a limited period of time. (Compl. ¶ 13). Moreover, plaintiff alleges that the defendants traded not only the same copyrighted work, but the same file of that work, as identified by the file’s hash number. (*Id.* ¶¶ 11, 13; Pl.’s Mem. of P. & A. at 5-6). Copyright Enforcement Group (“CEG”), a California company hired by Digital Sin to assist in enforcing its copyrights, was able to obtain the IP addresses of the Doe defendants at or about the time of the alleged infringement. (Nicolini Decl. ¶ 32). Using publicly available geolocation software, CEG further determined that the IP addresses very likely belong to individuals located in New York, and specifically in this District. (*Id.* ¶¶ 27, 29, 32-33; Compl. ¶ 14, Ex. D).

### DISCUSSION

In the last few years, copyright litigation involving the BitTorrent file-sharing protocol has proliferated in this District and elsewhere. Most courts have authorized the sort of expedited discovery being sought in this case to some degree. *See, e.g., Digital Sin, Inc. v. John Does 1-176*, — F.R.D. —, No. 12 Civ. 126 (AJN), 2012 WL 263491, at \*1, nn.1-2 (S.D.N.Y. Jan. 30, 2012) (Nathan, J.) (citing cases). But, at various stages in the litigation, courts have identified, and disagreed about, at least two legal issues presented by these cases — namely, the permissibility, under Rule 20 of the Federal Rules of Civil Procedure, of joining multiple Doe

defendants from the same BitTorrent “swarm” in a single suit; and whether the plaintiffs have pleaded sufficient facts to establish a *prima facie* case of personal jurisdiction over the Doe defendants given the means of identifying them. Before turning to Digital Sin’s request for expedited discovery in this case, the Court will briefly address these two issues.

With respect to joinder, Rule 20 allows defendants to be joined in a single suit if “any right to relief is asserted against them . . . arising out of the same transaction, occurrence, or series of transactions or occurrences.” Applying this Rule, many courts have concluded that where a plaintiff alleges a claim against members of the same BitTorrent “swarm,” the defendants are properly joined due to the interconnected nature of the BitTorrent protocol. *See, e.g., Digital Sin*, 2012 WL 263491, at \*5. Other courts have disagreed, concluding that defendants in BitTorrent cases “merely commit[ed] the same type of violation in the same way,” which would not make joinder proper. *E.g., Digital Sins, Inc. v. John Does 1-245*, No. 11 Civ. 8170 (CM), 2012 WL 1744838, at \*2 (S.D.N.Y. May 15, 2012) (McMahon, J.).

After careful review, this Court agrees with those courts that have concluded that where, as here, defendants are alleged to have copied a single work as part of the same “swarm” over a limited period of time, joinder is proper under Rule 20 — at least for this stage of the proceedings. As Judge Nathan explained in her own *Digital Sin* case, “it is difficult to see how the sharing and downloading activity alleged in the Complaint — a series of individuals connecting either directly with each other or as part of a chain or ‘swarm’ of connectivity designed to illegally copy and share the exact same copyrighted file — could *not* constitute a ‘series of transactions or occurrences’ for the purposes of Rule 20(a).” *Digital Sin*, 2012 WL 263491, at \*5 (emphasis in original). Nevertheless, like other courts that have allowed BitTorrent cases against Doe defendants to proceed, this Court remains open to reconsidering the

issue of joinder at a later date if raised by an ISP or defendant. Should an ISP or defendant raise different or conflicting defenses at a later date, the Court will also remain open to any request that it sever the claims against a particular defendant pursuant to Rule 21. The Court will consider the merits of any such request if or when it is made, and based upon the facts shown by the ISP or defendant. For present purposes, however, the Court concludes that Digital Sin has pleaded sufficient facts to allow defendants in this case to remain joined.

As noted, some courts have also addressed the issue of personal jurisdiction in cases involving BitTorrent, given the means by which the Doe defendants have been identified and joined. *See, e.g., Digital Sins, Inc.*, 2012 WL 1744838, at \*4-6; *see also Digiprotect USA Corp. v. John/Jane Does 1-240*, No. 10 Civ. 8760 (PAC), 2011 WL 4444666, at \*2-4 (S.D.N.Y. Sept. 26, 2011); *Digiprotect USA Corp. v. John/Jane Does 1-266*, No. 10 Civ. 8759 (TPG), 2011 WL 1466073, at \*3-4 (S.D.N.Y. Apr. 13, 2011). In the *Digiprotect* Cases, for example, Judges Griesa and Crotty rejected the plaintiffs' attempts to assert personal jurisdiction over defendants located around the country solely on the ground that they participated in a single swarm with a subset of defendants who resided in New York State. *See Digiprotect USA Corp.*, 2011 WL 4444666, at \*3; *Digiprotect USA Corp.* 2011 WL 1466073, at \*4. By contrast, most courts have held that a plaintiff succeeds in making out a *prima facie* case of personal jurisdiction where, relying on geolocation software that can identify the likely geographical locations of IP addresses, the plaintiff alleges that all defendants reside in the state within which the court is located. *See, e.g., Digital Sins*, 2012 WL 1744838 , at \*4 (citing cases).

This case is of the latter type. Specifically, relying on geolocation software, the plaintiff alleges that all Doe defendants reside in New York State, and more specifically within this District. (Compl. ¶ 2; Pl.'s Mem. of P. & A. at 5; Nicolini Decl. ¶ 27, 29, 32-33). Although this

technology does not allow for the determination of the Doe defendants' locations with absolute certainty (Meier V.S. (attached to Complaint) at 13; Nicolini Decl. ¶ 33), the Court concludes that these allegations are sufficient at this stage of the proceedings.<sup>1</sup> Furthermore, personal jurisdiction is a waivable defense, *see, e.g., City of New York v. Mickalis Pawn Shop, LLC*, 645 F.3d 114, 133 (2d Cir. 2011), and the Court will not presume that any of the Doe defendants will assert it. Accordingly, for present purposes, the Court holds that plaintiff has alleged sufficient facts to establish personal jurisdiction over defendants. As with joinder, however, the Court remains open to reconsideration of whether it has personal jurisdiction over any individual defendant upon a showing by that defendant that personal jurisdiction is lacking.

Having concluded that Digital Sin's allegations are sufficient for purposes of both joinder and personal jurisdiction at this stage of the proceedings, the Court turns to plaintiff's request for expedited discovery. Normally, parties are required to meet and confer prior to beginning any discovery. *See* FED. R. CIV. P. 26(d). Nevertheless, a court may waive this requirement by order. *See id.* For the most part, courts in this district have applied a "flexible standard of reasonableness and good cause" to determine whether expedited discovery is appropriate.

*Ayyash v. Bank Al-Madina*, 233 F.R.D. 325, 326-27 (S.D.N.Y. 2005) (Lynch, J.); *see also Stern v. Cosby*, 246 F.R.D. 453, 457 (S.D.N.Y. 2007) (Chin, J.); *accord* 8A CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2046.1 (3d ed. 2011) ("Although

---

<sup>1</sup> In her *Digital Sins* case, Judge McMahon expressed concerns about the manner in which counsel and CEG conducted the geolocation research on the Doe defendants as compared to the manner in which the research was conducted in Judge Nathan's *Digital Sins* case. *See* 2012 WL 1744838, at \*6. Specifically Judge McMahon expressed dismay that counsel appeared to have conducted geolocation tests on only a batch of the Doe defendants. Whatever happened in these other cases, it is clear from the pleadings in this case that plaintiff's technology consultant conducted geolocation tests on *all* of the Doe defendants, a random batch of which were checked by plaintiff's counsel to ensure accuracy. (Meier V.S. at 13, Compl. Ex. D; Nicolini Decl. ¶¶ 27-29, 32). The Court finds that this methodology is sufficient for present purposes.

[Rule 26(d)] does not say so, it is implicit that some showing of good cause should be made to justify such an order, and courts presented with requests for immediate discovery have frequently treated the question whether to authorize early discovery as governed by a good cause standard.”). *But see Notaro v. Koch*, 95 F.R.D. 403, 405 & n.4 (S.D.N.Y. 1982) (applying a four-part test more akin to the preliminary injunction standard).

Applying that standard here, the Court concludes that plaintiff has established the need for expedited discovery. Digital Sin has alleged a *prima facie* case of infringement, and the combination of (1) the anonymous nature of the BitTorrent file-sharing protocol and (2) statutory provisions requiring the ISPs to maintain their customers’ privacy leaves no alternative means of identifying the alleged infringers. *See Digital Sin*, 2012 WL 263491, at \*2 (citing 47 U.S.C. §§ 522(5), 551(c)). Expedited discovery is also necessary to prevent loss of the requested information as a result of routine deletion by the ISPs. (Nicolini Decl. ¶ 37). In short, expedited discovery is the only means by which Digital Sin can identify those who allegedly violated its copyright in the Video. Accordingly, this Court finds that plaintiff has established good cause to issue Rule 45 subpoenas to the ISPs listed in Exhibit A to the Complaint.

The Court finds, however, that there is also good cause to issue a protective order in connection with this discovery. Pursuant to Rule 26(c)(1) of the Federal Rules of Civil Procedure, a district court has authority to issue a protective order, based upon good cause, to protect parties from “annoyance, embarrassment, oppression, or undue burden or expense[.]” In another Digital Sin case brought by the same counsel as in this case, counsel conceded that there was a high risk of false positive identifications (that is, as many as “30% of the names turned over by the ISPs may not be those of individuals who actually downloaded or shared copyrighted material”) and that there were “horror stories” of harassing and abusive litigation techniques by

some law firms. *See Digital Sin*, 2012 WL 263491 at \*3. The combination of these factors and the nature of the copyrighted work in this case creates the possibility of undue embarrassment and harm were a Doe defendant's name to be publicly, but erroneously, linked to the illegal downloading of the plaintiff's copyrighted work. Accordingly, the Court finds that there are sufficient grounds to issue a protective order to protect against these concerns.

### CONCLUSION

For the foregoing reasons, it is hereby **ORDERED** that plaintiff may immediately serve a Rule 45 subpoena on the ISPs listed in Exhibit A to the Complaint to obtain information to identify Does 1-27, specifically his or her name, current and permanent address, and Media Access Control address. Plaintiff is expressly *not* permitted to subpoena the ISPs for the Doe defendants' email addresses or telephone numbers.

It is further **ORDERED** that plaintiff shall serve a copy of this Opinion and Order as well as the attached "Notice to Defendants" along with any subpoenas to the listed ISPs.

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 the relevant Does with a copy of the subpoena, a copy of this Opinion and Order, and a copy of the "Notice to Defendants." *The Opinion and Order should be attached to the "Notice to Defendants" such that the "Notice to Defendants" is the first page of the materials enclosed with the subpoena.* The ISPs may serve the Does using any reasonable means, including written notice sent to his or her last known address, transmitted either by first-class mail or via overnight service.

It is further **ORDERED** that each Doe defendant shall have *60 days* from the date of service of the Rule 45 subpoena and this Opinion and Order upon him or her 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. Additionally, if a defendant or ISP files a motion to quash or modify the subpoena, or a request to litigate the subpoena anonymously, the ISPs may not turn over any information to plaintiff until the issues have been addressed and the Court issues an order instructing the ISPs to resume in turning over the requested discovery.

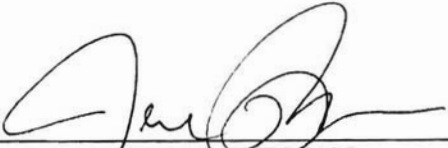
It is further **ORDERED** that the subpoenaed entity shall preserve any subpoenaed information pending the resolution of any timely filed motion to quash.

It is further **ORDERED** that an ISP that receives a subpoena pursuant to this Opinion and 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 solely for the purpose of protecting plaintiff's rights as set forth in its complaint.

SO ORDERED.

Dated: June 6, 2012  
New York, New York



JESSE M. FURMAN  
United States District Judge

**Notice to Defendants in *Digital Sin v. John Does 1-27***

1. You are a defendant in *Digital Sin v. John Does 1-27*, 12 Civ. 3873 (JMF), a case now pending before the Honorable Jesse M. Furman, United States District Judge for the Southern District of New York.
2. Attached is Judge Furman's Order, dated June 6, 2012, which sets forth certain deadlines and procedures related to this case.
3. You may hire a lawyer to represent you in this case or you may proceed *pro se* (that is, you may represent yourself without the assistance of a lawyer). If you choose to proceed *pro se*, all communications with the Court should be through the *Pro Se* Office of the United States District Court for the Southern District of New York. The *Pro Se* Office is located in Room 230 of the United States Courthouse, 500 Pearl Street, New York, NY 10007, and may be reached at (212) 805-0175.
4. The plaintiff in this case has filed a lawsuit claiming that you have illegally downloaded and/or distributed a movie on your computer.
5. The plaintiff may not know your actual name or address, but it does know the Internet Protocol address ("IP address") of the computer associated with the alleged downloading and/or distributing.
6. The plaintiff has filed subpoenas requesting your identity and contact information from your Internet Service Provider ("ISP").
7. If you do not want your ISP to provide this information to the plaintiff and you believe there is a legal basis for the ISP to withhold the information, you may file a motion to "quash" or "modify" the subpoena. This must be done within 60 days of the date that you receive notice from your ISP that you are a defendant in this case.
8. If you move to quash the subpoena or otherwise move to prevent your name from being turned over to the plaintiff, you may proceed anonymously at this time. Nevertheless, if you are representing yourself, you will have to complete an information card that you can obtain from the *Pro Se* Office of the Court. This information is *solely for use by the Court* and the Court will not provide this information to lawyers for the plaintiff unless and until it determines there is no basis to withhold it. The Court must have this information so that it may communicate with you regarding the case.
9. Even if you do not file a motion to quash or modify the subpoena, you may still proceed in this case anonymously at this time. This means that the Court and the plaintiff will know your identity and contact information, but your identity will not be made public unless and until the Court determines there is no basis to withhold it.
10. If you want to proceed anonymously without filing a motion to quash or modify the subpoena, you (or, if represented, your lawyer) should provide a letter stating that you would like to proceed anonymously in your case. This must be done within 60 days of the date that you receive notice from your ISP that you are a defendant in this case. You should identify yourself in your letter by the case in which you are a defendant, your IP address, and your "Doe number." The Doe number is the number associated with your IP address; this number should have been provided to you by your ISP, but if it has not then you need only identify yourself by your IP address and the name and number of the case in which you are a defendant. If you submit this letter, then your identity and contact information will not be revealed to the public unless and until the Court says otherwise.