

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

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

Plaintiff, :

-v- :

JOHN DOES 1-176 :

Defendants. :

12-CV-00126 (AJN)

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

----- X
ALISON J. NATHAN, District Judge:

Plaintiff Digital Sin, Inc. (“Digital Sin”) filed an *ex parte* motion seeking permission to take expedited discovery from third-party Internet Service Providers (“ISPs”) to identify the names, physical addresses, e-mail addresses, and Media Access Control (“MAC”) addresses associated with identified Internet Protocol (“IP”) addresses that Digital Sin alleges were used to illegally share its copyrighted motion picture in violation of 17 U.S.C. § 101 *et seq.*

Litigation of this nature, involving *ex parte* applications for expedited discovery of identifying information pertaining to hundreds or thousands of John Doe defendants, is proliferating in this district and throughout the country. Some courts, faced with these *ex parte* applications for expedited discovery, have expressed serious concerns about the nature of the litigation and have denied the *ex parte* applications or severed all but one of the Doe defendants.¹ Other courts have granted the applications and issued orders allowing the expedited discovery to proceed in order to identify the Doe defendants.²

¹ See, e.g., *SBO Pictures, Inc. v. Does 1-3036*, 2011 WL 6002620 (N.D. Cal. Nov. 30, 2011) (severing and permitting expedited discovery as to the identity of one Doe

This Court has serious reservations about the *ex parte* application and the proposed order submitted by the Plaintiff. Nevertheless, for the reasons discussed below, the Court finds that good cause exists for Digital Sin to engage in cabined expedited discovery with respect to the IP addresses listed in Exhibit A to its Complaint (Docket #1), but only pursuant to a protective order as outlined in Section III.

I. Background

Digital Sin is a California company that produced a motion picture titled “My Little Panties #2” (“Motion Picture”). Digital Sin alleges the following facts in its Complaint, memorandum of law and accompanying declaration. The Court, while making no findings, accepts these facts as true for purposes of this ruling.

Digital Sin contracted “Copyright Enforcement Group” (“CEG”), a company that discovers copyright infringements and arranges for enforcement (Nicolini Dec. ¶ 3). CEG determined that a number of individuals were sharing the Motion Picture using an internet protocol called BitTorrent. (Comp. ¶¶ 12; Nicolini Dec. ¶¶ 9–17). BitTorrent software allows users to join together in a “peer-to-peer” network to download and make

defendant pursuant to a protective order); *Digital Sin, Inc. v. Does 1–5698*, 2011 WL 5362068 (N.D. Cal. Nov. 4, 2011) (same); *Hard Drive Prods., Inc. v. Does 1–30*, 2011 WL 4915551 (E.D. Va. Oct. 17, 2011) (severing and ordering plaintiff’s counsel to show cause as to why materials gained by Rule 45 subpoenas issued in previous, analogous cases should not be “suppressed”); *Digiprotect USA Corp. v. Does 1–240*, 2011 WL 4444666, at *2–4 (S.D.N.Y. Sept. 26, 2011) (finding joinder improper based on facts pleaded in initial Complaint).

² See, e.g., *Call of the Wild Movie, LLC v. Does 1–1,062*, 770 F. Supp. 2d 332 (D.D.C. 2011); *K-Beech, Inc. v. Does 1–57*, 2011 WL 5597303 (M.D. Fla. Nov. 1, 2011); *MCGIP, LLC v. Does 1–18*, 2011 WL 2181620 (N.D. Cal. June 2, 2011); *Voltage Pictures, LLC v. Does 1–5,000*, 2011 WL 1807438 (D.D.C. May 12, 2011); *First Time Videos, LLC v. Does 1–76*, 276 F.R.D. 254 (N.D. Ill. 2011); see also Order Permitting Expedited Discovery, *Media Prods., Inc. v. Does 1–59*, 12-CV-125 (S.D.N.Y. Jan. 11, 2012); Order Permitting Expedited Discovery, *Next Phase Distrib., Inc. v. Does 1–138*, 11-CV-9706 (S.D.N.Y. Jan. 6, 2012); Order Permitting Expedited Discovery, *Patrick Collins, Inc. v. Does 1–115*, 11-CV-9705 (S.D.N.Y. Jan. 5, 2012).

available for download large files. (Nicolini Dec. ¶¶ 5–7). The individual downloaders might only download small pieces of the file at a time and it may take several days or even weeks for an individual to download an entire file. (1/17/12 Tr. at 10). While downloading, the downloader is also required to share with others the pieces of the file that she or he has already successfully downloaded. (*Id.* at 13–14). This group of interacting users is referred to as a “swarm.” (Nicolini Dec. ¶ 6).

Individuals who participate in a swarm expose the IP address they are using when downloading or sharing a file. (Comp. ¶ 12). As a result, CEG was able to obtain 176 IP addresses that were being used to share and download the same Motion Picture file without permission. (*Id.*). Publicly available “reverse IP” checks confirmed that all of these addresses very likely belong to individuals located in New York. (Comp. ¶ 14).³

Immediately after initiating its complaint against the 176 John Doe defendants, identifying them by their IP addresses, Digital Sin filed an *ex parte* motion for expedited discovery seeking access to the names and addresses of the individuals affiliated with the IP addresses as found in the ISPs’ account records. Plaintiff alleges that this account information may be routinely erased by ISPs and therefore lost forever if Plaintiff’s motion is not granted on an expedited basis. (Nicolini Dec., ¶ 27). In response to Plaintiff’s *ex parte* motion, the Court ordered an *ex parte* conference call with Plaintiff’s

³ This factual assertion by Plaintiff as to the location of the Doe defendants at the time of the alleged infringement is critical for establishing that personal jurisdiction is proper in this Court. *See Digiprotect USA Corp. v. Does 1–266*, 2011 WL 1466073, at *3–4 (S.D.N.Y. April 13, 2011); *see also Digiprotect USA Corp. v. Does 1–240*, 2011 WL 4444666, at *2–4 (S.D.N.Y. Sept. 26, 2011). Should the ISPs or any Doe defendants make a showing that undermines this factual assertion, the Court will of course reassess the issue of personal jurisdiction.

counsel on January 17, 2012. Plaintiff's counsel was asked to address the Court's concerns regarding privacy, joinder, and the potential for misidentification of defendants.

II. Discussion

A. Good Cause Standard

Though parties generally may not initiate discovery prior to satisfying the meet and confer requirement of Fed. R. Civ. P. 26(f), courts may in some instances order earlier discovery. Fed. R. Civ. P. 26(d). Courts in this district have applied a "flexible standard of reasonableness and good cause" in determining whether to grant a party's expedited discovery request. *Ayyash v. 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 [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."). Courts have also applied "particularly careful scrutiny" when plaintiffs seek expedited discovery on an *ex parte* basis. *Ayyash*, 233 F.R.D. at 327.

Here, Plaintiff has alleged a *prima facie* case of infringement sufficient for purposes of this motion and appears to have no other way of obtaining the identities of the alleged infringers. Absent a Court-ordered subpoena, many of the ISPs, who qualify as "cable operators" for purposes of 47 U.S.C. § 522(5), are effectively prohibited by 47 U.S.C. § 551(c) from disclosing the identities of the putative defendants to Plaintiff. Indeed, in all of the opinions and rulings in similar cases around the country, the Court

has found no indication that the plaintiffs have any reasonable alternative to these subpoenas to obtain the identities of the alleged infringers. Thus, without granting Plaintiff's request, the defendants cannot be identified or served and the litigation cannot proceed. Additionally, expedited discovery is necessary to prevent the requested data from being lost forever as part of routine deletions by the ISPs.

Under these circumstances, the Court finds that Plaintiff has established good cause to issue a Rule 45 subpoena to the ISPs listed in Exhibit A to its Complaint (Docket #1) to obtain the name, physical address, e-mail address, and MAC address associated with each defendant IP address subject to the protective order outlined in Sections II.B and III below.

B. Protective Order

District courts may for good cause issue a protective order to spare parties "annoyance, embarrassment, oppression, or undue burden." Fed. R. Civ. P. 26(c)(1). Plaintiff's counsel stated that he will not object to allowing defendants to litigate the matter anonymously, nor will he object to language in an order informing defendants of their ability to do so. (1/17/12 Tr. at 17).

The Court is concerned about the possibility that many of the names and addresses produced in response to Plaintiff's discovery request will not in fact be those of the individuals who downloaded "My Little Panties #2." The risk is not purely speculative; Plaintiff's counsel estimated that 30% of the names turned over by ISPs are not those of individuals who actually downloaded or shared copyrighted material. Counsel stated that the true offender is often the "teenaged son . . . or the boyfriend if it's a lady." (1/17/12 Tr. at 16). Alternatively, the perpetrator might turn out to be a

neighbor in an apartment building that uses shared IP addresses or a dormitory that uses shared wireless networks. *See, e.g.,* Mot. to Quash Verizon Subpoena, 11-CV-7564 (S.D.N.Y. Jan. 6, 2012) (Docket #11) (claiming that a Doe defendant did not know how to use a computer and implying that the perpetrator was a neighbor in his condominium). This risk of false positives gives rise to “the potential for coercing unjust settlements from innocent defendants” such as individuals who want to avoid the embarrassment of having their names publicly associated with allegations of illegally downloading “My Little Panties #2.” *SBO Pictures, Inc. v. Does 1–3036*, 2011 WL 6002620, at *4 (N.D. Cal. Nov. 30, 2011).

One court in Virginia recently described this dynamic as follows:

According to some of the defendants, [following the Court’s grant of expedited discovery compelling the ISPs to turn over the names associated with 85 IP addresses,] the plaintiffs then contacted the John Does, alerting them to this lawsuit and their potential liability. Some defendants have indicated that the plaintiff has contacted them directly with harassing telephone calls, demanding \$2,900 in compensation to end the litigation

This course of conduct indicates that the plaintiffs have used the offices of the Court as an inexpensive means to gain the Doe defendants’ personal information and coerce payment from them. The plaintiffs seemingly have no interest in actually litigating the cases, but rather **simply have used the Court and its subpoena powers to obtain sufficient information to shake down the John Does.**

K-Beech, Inc. v. Does 1–85, 11-CV-00469 at 4 (E.D. Va. Oct. 5, 2011) (Docket #9) (severing Doe defendants and issuing an Order To Show Cause demanding that attorney for plaintiff explain why Rule 11 sanctions were inappropriate) (emphasis added and internal citations omitted). Indeed Plaintiff’s counsel also bluntly conceded that there are “horror stories out there, what some law firms have done. For example, they have

called and harassed the John Doe defendants.” (1/17/12 Tr. at 20). The Court appreciates counsel’s candor and notes that Plaintiff’s counsel appropriately does not request that the ISPs turn over the John Does’ telephone numbers.

Accordingly, the Court **will issue a protective order** to the extent that any information regarding the Doe defendants released to Digital Sin by the ISPs shall be treated as confidential for a limited duration. This Order is adapted from the one issued by Magistrate Judge Beeler in *Digital Sin, Inc. v. Does 1-5698*, 2011 WL 5362068 (N.D. Cal. Nov. 4, 2011) and outlined in Section III below. At base, the protective order allows Doe defendants and the ISPs to be heard in this matter before the identifying information is revealed to Plaintiff.

C. Joinder of 176 Doe Defendants Pursuant to Rule 20(a)

The Court finally turns to the difficult question of whether the 176 Doe defendants are properly joined into this single action pursuant to Rule 20(a)(2). Parties may be joined when (1) the defendants are jointly and severally liable under the claims asserted by the plaintiff, or (2) the claims for relief by the plaintiff arises out of the same transaction, occurrence, or series of transactions or occurrences. Fed. R. Civ. P. 20(a)(2). Additionally, there must be common questions of law or fact. *Id.* 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.” *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 724 (1966); “The purpose of the rule is to promote trial convenience and expedite the final determination of disputes, thereby preventing multiple lawsuits.” 7 Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 1652 (3d ed. 2011). “District

Courts have broad discretion to determine whether or not to grant a motion to sever.” *In re WorldCom, Inc. Sec. Litig.*, 2003 WL 1563412, at *3 (S.D.N.Y. March 25, 2003) (Cote, J.).

Though Plaintiff did not cite or distinguish them in its *ex parte* motion papers, the Court has become aware of several analogous copyright infringement cases from across the country finding it improper under Fed. R. Civ. P. 20(a) to join into one action hundreds (or in some cases thousands) of Doe defendants.⁴ At the same time, several courts have drawn the opposite conclusion, finding joinder to be proper under similar circumstances.⁵

During the January 17, 2011, *ex parte* conference, Plaintiff argued that the cases finding joinder of so many Doe defendants improper in copyright infringement cases were distinguishable because they involved substantially more defendants from different geographic areas lumped together into one action, as well as users accessing the same copyrighted work through different files available from different swarms. (1/17/12 Tr. at 5–8, 10–11). In the present action, Plaintiff claims to have carefully selected only a small group of New York-based defendants who traded the exact same file, identifiable by a hash value, as part of the same swarm within a six-week period. (*Id.*).

Yet Magistrate Judge Spero in the Northern District of California, assessing a situation identical to the present case where joined defendants were part of the same BitTorrent “swarm,” wrote:

⁴ See, e.g., *supra* note 1.

⁵ See, e.g., *Call of the Wild Movie, LLC v. Does 1–1,062*, 770 F. Supp. 2d 332 (D.D.C. 2011); *K-Beech, Inc. v. Does 1–57*, 2011 WL 5597303 (M.D. Fla. Nov. 1, 2011); *MCGIP, LLC v. Does 1–18*, 2011 WL 2181620 (N.D. Cal. June 2, 2011); *Voltage Pictures, LLC v. Does 1–5,000*, 2011 WL 1807438 (D.D.C. May 12, 2011); *First Time Videos, LLC v. Does 1–76*, 276 F.R.D. 254 (N.D. Ill. 2011).

Under the BitTorrent Protocol, it is not necessary that each of the Does 1–188 participated in or contributed to the downloading of each other’s copies of the work at issue—or even participated in or contributed to the downloading by any of the Does 1–188. Any ‘pieces’ of the work copied or uploaded by any individual Doe may have gone to any other Doe [but also] *to any of the potentially thousands who participated in a given swarm.*

Hard Drive Prods., Inc., 2011 WL 3740473, at *13 (N.D. Cal. Aug. 23, 2011) (emphasis in original). Magistrate Judge Spero concluded that this pattern of usage did not amount to the same transaction, occurrence, or series of transactions or occurrences, for purposes of Rule 20. *Id.*

Judge Crotty came to a different conclusion in *Digiprotect USA Corp. v. Does 1–240*, 2011 WL 4444666 (S.D.N.Y. Sept. 26, 2011). In *Digiprotect*, the plaintiff alleged that Doe defendants across the country traded the same copyrighted work, but as parts of different swarms, utilizing different file sharing software and networks. *Digiprotect* Complaint at ¶¶ 9–10, No. 10-CV-8760 (S.D.N.Y. Nov. 19, 2010) (Docket #1).

Although he dismissed the case on jurisdictional grounds, Judge Crotty also instructed that any re-pleading “must be based on specific allegations connecting the[] defendants to the same specific swarming transaction, or series of transactions, to support their joinder.” *Digiprotect*, 2011 WL 4444666, at *3 n.3.

This Court is persuaded to adopt the standard articulated by Judge Crotty in *Digiprotect*. In particular, 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 purposes of Rule 20(a). In the present case, Plaintiff has satisfied the *Digiprotect* standard by alleging that the Doe defendants were trading the exact same file as part of the same swarm. As a result, the Court declines to sever the case at this time. *See MCGIP, LLC v. Does 1–18*, 2011 WL 2181620, at *1 (N.D. Cal. June 2, 2011) (“[A]ssertion of improper joinder may be meritorious but, at this stage in the litigation, when discovery is underway only to learn identifying facts necessary to permit service on Doe defendants, joinder of unknown parties identified only by IP addresses is proper”) (internal citations and quotation marks omitted).⁶

The Court remains open, however, to reconsidering this issue at a later date. Should John Doe defendants come forward to defend themselves against the allegations in the Complaint—potentially raising differing, conflicting defenses—the Court will remain open to any arguments against joinder of the parties that those defendants wish to make at that time. The Court will also remain open to hearing arguments regarding joinder or any other matters from the ISPs, should they move to quash Digital Sin’s Rule 45 subpoena. The Court simply holds that for purposes of carrying out the initial, necessary discovery in an efficient manner, the claims may remain joined together at this time.

⁶ The Court is also cognizant of other considerations that have caused some courts not to sever, including that severance at this stage in the litigation would introduce “significant obstacles in [plaintiffs’] efforts to protect their copyrights from illegal file-sharers and this would only needlessly delay their cases.” *Call of the Wild Movie, LLC v. Does 1–1,062*, 770 F. Supp. 2d 332, 344 (D.D.C. 2011). Furthermore, courts have opined that requiring aggrieved parties to file hundreds or even thousands of separate copyright infringement actions would neither be cost efficient for the plaintiffs nor promote convenience or judicial economy for the courts. *See, e.g., id.* at 344–45.

III. Conclusion

IT IS HEREBY ORDERED that Digital Sin may immediately serve a Rule 45 subpoena on the ISPs listed in Exhibit A to the Complaint to obtain information to identify Does 1–176, specifically her or his name, address, MAC address, and email address. The subpoena shall have a copy of this order attached.

IT IS FURTHER ORDERED that the ISP will have *60 days* from the date of service of the Rule 45 subpoena upon them to serve Does 1–176 with a copy of the subpoena and a copy of this order. The ISPs may serve Doe 1–176 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 1–176 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 Digital Sin before the expiration of this 60-day period. Additionally, if a defendant or ISP files a motion to quash the subpoena, the ISPs may not turn over any information to Digital Sin 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 if that 60-day period lapses without a Doe defendant or ISP contesting the subpoena, the ISPs shall have *10 days* to produce the information responsive to the subpoena to Plaintiff. **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' contact information to Plaintiff until the Court rules on any such motions.

IT IS FURTHER ORDERED that the subpoenaed entity shall preserve any subpoenaed information pending the resolution of any timely-filed motion to quash.

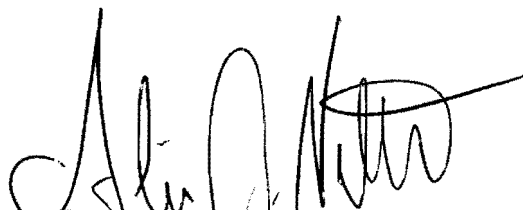
IT IS FURTHER ORDERED that an ISP that receives a subpoena pursuant to this order shall confer with Digital Sin and shall not assess any charge in advance of providing the information requested in the subpoena. An ISP that receives a subpoena and elects to charge for the costs of production shall provide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

IT IS FURTHER ORDERED that Digital Sin shall serve a copy of this Opinion and Order along with any subpoenas issued pursuant to this order to the listed ISPs.

IT IS FURTHER ORDERED that any information ultimately disclosed to Digital Sin in response to a Rule 45 subpoena may be used by Digital Sin solely for the purpose of protecting Digital Sin's rights as set forth in its complaint.

SO ORDERED:

Dated: *JAN. 30, 2012*
New York, New York


ALISON J. NATHAN
United States District Judge