

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X

DIGITAL SIN, INC.  
21345 Lassen St.  
Chatsworth, CA 91311,

No. 12-cv-3873 (JMF)

Plaintiff,

-against-

**NOTICE OF  
MOTION**

DOES 1-27,

Defendants.

-----X

PLEASE TAKE NOTICE that, upon the annexed affidavit of Morlan Ty Rogers, Esq. and the exhibits annexed hereto, the accompanying Memorandum of Law, and all prior papers and proceedings herein, and pursuant to the fourth decretal paragraph on pages 8-9 of the Court's June 6, 2012 *ex parte* discovery order, the undersigned hereby moves before the Honorable Jesse M. Furman, United States District Judge, in Courtroom 26A of the United States District Court for the Southern District of New York, 500 Pearl Street, New York, New York 10007, for an Order dismissing the complaint herein pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure and quashing the subpoenas issued under the Court's June 6, 2012 *ex parte* discovery order seeking disclosure of defendants' identities on the ground that the complaint herein fails to state a claim, and granting such other and further relief as may be just and proper.

PLEASE TAKE FURTHER NOTICE that opposing affidavits and memoranda of law, if any, must be served and filed with the Court on or before August 31, 2012. Unless such affidavits and memoranda of law are timely served and filed, the relief sought herein may be granted.

Dated: Forest Hills, New York  
August 17, 2012

RAY BECKERMAN, P.C.

By:       s/Morlan Ty Rogers  
Morlan Ty Rogers (MR 3818)  
Attorneys for defendant Doe No. 1  
108-18 Queens Blvd., 4<sup>th</sup> Floor  
Forest Hills, NY 11375  
(718) 544-3434

To: Mike Meier, Esq.  
The Copyright Law Group, PLLC  
Attorneys for plaintiff  
4000 Legato Road, Suite 1100  
Fairfax, VA 22033  
(888) 407-6770

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----x

No. 12-cv-3873 (JMF)

DIGITAL SIN, INC.  
21345 Lassen St.  
Chatsworth, CA 91311,

Plaintiff,

**AFFIDAVIT**

-against-

DOES 1-27,

Defendants.

-----x

STATE OF NEW YORK     )  
  ) ss.:  
COUNTY OF QUEENS     )

MORLAN TY ROGERS, being duly sworn, deposes and says:

1. I am a member of the bar of this Court and Of Counsel to Ray Beckerman, P.C., attorneys for defendant Doe No. 1 (“Doe 1”), and respectfully submit this affidavit in support of his motion for an Order dismissing the complaint herein pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure and quashing the subpoenas issued under the Court’s June 6, 2012 *ex parte* discovery order seeking disclosure of defendants’ identities on the ground that the complaint herein fails to state a claim.

2. I know the identity of Doe 1, who wishes to remain anonymous.

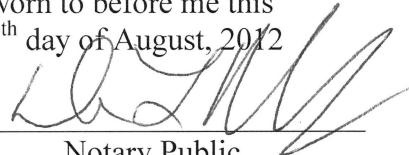
3. Annexed hereto as Exhibit “A” is a copy of plaintiff’s complaint herein. Annexed hereto as Exhibit “B” is the list of Doe defendants and IP addresses that plaintiff filed along with the complaint. Annexed hereto as Exhibit “C” is a copy of the

*ex parte* discovery order. Annexed hereto as Exhibit "D" is a copy of the notice and subpoena served by Plaintiff's counsel upon Doe 1's internet service provider, Verizon, pursuant to said *ex parte* discovery order and subsequently forwarded to Doe 1.

4. For the reasons set forth in the accompanying memorandum of law, the Court should grant the within motion in all respects.

  
MORLAN TY ROGERS

Sworn to before me this  
17<sup>th</sup> day of August, 2012

  
Notary Public

DIANE NICKELBERG  
Notary Public, State of New York  
No. 01-NI4959042  
Qualified in Queens County  
Commission Expires Nov. 28, 2013



Defendants identified reside or can be found in the geographic area of this Court. As explained below and in the attached *Declaration of Jon Nicolini*, Plaintiff has used its best efforts to identify Defendants only in the geographic location of the Court, and has cross-referenced the data with commercially available databases to ensure that all Defendants reside in the District. Such technology to identify the location of such Defendants is considered very accurate, but not necessarily accurate in all cases.

3. On information and belief, personal jurisdiction in this District is proper because each Defendant, without consent or permission of Plaintiff as the exclusive rights owner, intentionally and willfully distributed, and offered to distribute over the Internet, copyrighted works for which Plaintiff has exclusive rights. In addition, each Defendant contracted with an Internet Service Provider (ISP) found in this District to provide each Defendant with access to the Internet. Therefore, venue in this Court is proper in accordance with 28 U.S.C. 1400(a).

4. To ensure that venue and jurisdiction are proper, Plaintiff, through its agents and representatives, has undertaken efforts to only identify alleged infringers who are within or near the geographic location of the Court. *See attached Declaration of Jon Nicolini, Exhibit B; see Listing of the believed State and County of Residence for each John Doe, Exhibit D.*

### **JOINDER**

5. Pursuant to Fed.R.Civ.P. 20(a)(2), the Defendants have been properly joined, as set forth in detail below and in Exhibit B, because Plaintiff alleges that all Defendants have traded (uploaded and downloaded) the exact same file of the copyrighted works in related transactions through torrent software. The Defendants were identified through the use of forensic software. Plaintiff, through its agents and representatives, has taken steps to confirm that all

Defendants have in fact engaged in a series of related transactions or occurrences. All Defendants identified in Exhibit A (i) have traded exactly the same file of the copyrighted work as shown by the identical hash mark; (ii) have traded (simultaneously uploaded and downloaded) the exact same file as is the nature of torrent software; and (iii) the alleged events occurred within a limited period of time. *See attached Declaration of Jon Nicolini, Exhibit B.* Further, Plaintiff has used its best efforts to only identify Defendants who are within the geographic location of the Court, as explained in the Complaint and the *Declaration of Jon Nicolini*. *See attached Declaration of Jon Nicolini, Exhibit B; see also Listing of the believed State of Residence for each John Doe, Exhibit D.*

#### GENERAL ALLEGATIONS

6. Plaintiff Digital Sin, Inc., is a corporation duly formed and existing under the laws of California, and has a principal place of business at 21345 Lassen St., Chatsworth, CA 91311.

7. The true names of Defendants are unknown to the Plaintiff at this time. Each Defendant is known to Plaintiff only by the Internet Protocol (“IP”) address assigned to that Defendant by his, her or its Internet Service Provider on the date and at the time at which the infringing activity of each Defendant was observed. The IP address of each Defendant, together with the date and time at which his, her or its infringing activity was observed and the hash value of the file, is included on **Exhibit A** which is attached hereto. The technology used to identify each Defendant is explained in **Exhibit B**. On information and belief, Plaintiff states that information obtained in discovery will lead to the identification of each Defendants’ true names and addresses and will permit Plaintiff to amend this Complaint to state the same.

8. The Motion Picture at issue (the “Motion Picture”) is identified in this Complaint only by the file number of the U.S. Copyright Office. It was produced by Plaintiff and released

on January 19, 2012. The copyright was applied for on January 23, 2012, the Service Request Number is 1-714915653. **See Exhibit C.** It is offered as a DVD through various vendors, including [www.cduniverse.com](http://www.cduniverse.com) for \$22.89.

9. The torrent protocol makes home computers with low bandwidth capable of participating in large data transfers across so-called “Peer-to-Peer” (P2P) networks. The first file-provider decides to share a file (“seed”) with a torrent network. Then other users (“peers”) within the network connect to the seed file for downloading. As additional peers request the same file, they become part of the same network. Unlike a traditional P2P network, each new peer receives a different piece of the data from each peer who has already downloaded the file. This system of multiple pieces of data coming from peers is called a “swarm.” As a result, every downloader is also an uploader of the illegally transferred file and is simultaneously taking copyrighted material through many ISPs in numerous jurisdictions around the country.

10. Once a participant in these downloading and uploading transactions becomes a peer, the software reassembles the file and the peer can view the Motion Picture. Once a peer has downloaded the complete file, that peer becomes an additional seed because he or she continues to distribute the torrent file (here: the copyrighted work).

11. In this case, all Defendants have not only swapped the same copyrighted work, they have traded the exact same file. The devices connected to all IP addresses identified in Exhibit A have utilized the same exact hash mark (a 40-character hexadecimal string which through cryptographic methods clearly identifies the Release, comparable to a forensic digital fingerprint) which establishes them as having taken part in the same series of transactions. All alleged infringers downloaded the exact same copyrighted work while trading in the same torrent.



12. While Defendants engaged in this downloading and/or uploading of the file, they exposed their IP address to the public. With torrent software, one can see the IP address of the various computers that one is connected to, and which are sharing files in cooperation with, one's own computer.

13. Through the use of torrent technology, the Defendants in this case engaged in deliberate distribution of unlawful copies of the Motion Picture. Moreover, the Defendants in this case engaged in a series of related transactions, because they all downloaded the exact same file (not just the same copyrighted work), within a limited period of time. Furthermore, because of the nature of torrent software, they engaged in a series of related transactions because in order to download a movie (or parts of it), one must permit other users to download and/or upload the file from one's own computer. Thus, the Defendants were simultaneously trading (downloading and/or uploading) the exact same file during a limited period of time.

14. By using geo-location technology and referencing the tracking data with other databases, Plaintiff has attempted to ensure that the IP addresses are likely within the geographic location of the Court. *See attached Listing of the believed State of Residence for each John Doe, Exhibit D.*

Plaintiff has used its best efforts to only identify Defendants who are within the geographic location of the Court, as explained in the Complaint and the *Declaration of Jon Nicolini*. The time period during which the identified illegal downloads occurred is limited to ensure commonality amongst the Defendants. The Defendants so identified downloaded the identical copyrighted work as part of the same series of transactions or occurrences and are thus specifically and directly related.

**COUNT I**

**COPYRIGHT INFRINGEMENT UNDER 17 U.S.C. §§ 101 ET SEQ.**

15. Plaintiff repeats and reincorporates herein the allegations set forth in paragraphs 1-14, above.

16. Plaintiff is a motion picture production company. Plaintiff is, and at all relevant times has been, the owner of the copyrights and/or the owner of the exclusive rights under the copyrights in the United States in the Motion Picture at issue.

17. The Motion Picture is an original work that is copyrighted under United States law. The Motion Picture is the subject of a Copyright Registration, and Plaintiff owns that registration. The title of the Motion Picture and its copyright registration number are included in **Exhibit C**. Thus, Plaintiff is entitled to statutory remedies of the U.S. Copyright Act.

18. Plaintiff has either published or licensed for publication all copies of the Motion Picture in compliance with the copyright laws.

19. **Exhibit A** identifies each Defendant (one Defendant per row in the table set out in **Exhibit A**) that has, without the permission or consent of the Plaintiff, reproduced and distributed to the public at least a substantial portion of the Motion Picture. That is, each Defendant listed in **Exhibit A** has, without permission or consent of Plaintiff, reproduced and distributed to the public at least a substantial portion of Plaintiff's copyrighted Motion Picture.

20. **Exhibit A** also sets out the Internet Protocol ("IP") address associated with each respective Defendant, the identity of the Internet Service Provider (often referred to as an "ISP") associated with the IP address, the last-observed date and time ("Timestamp") that the infringement by that Defendant of Plaintiff's copyright in the Motion Picture was observed and

the software protocol used by the Defendant. It also shows the hash value of the file so traded, which shows that each Defendant traded exactly the same file.

21. Further, Plaintiff is informed and believes that each of the Defendants, without the permission or consent of Plaintiff, has used, and continues to use, an online media distribution system (sometimes referred to as a "peer to peer" network or a "P2P" network) to reproduce at least one copy of the Motion Picture, and to distribute to the public, including by making available for distribution to others, copies of the Motion Picture. In doing so, each Defendant has violated, and continues to violate, Plaintiff's exclusive rights of reproduction and distribution protected under the Copyright Act of 1976 (17 U.S.C. § 101 et seq.), including under 17 U.S.C. § 106(1) and (3).

22. Each Defendant has acted in cooperation with the other Defendants by agreeing to provide, and actually providing, on a P2P network an infringing reproduction of at least substantial portions of Plaintiff's copyrighted Motion Picture, in anticipation of the other Defendants doing likewise with respect to that work and/or other works. Further in this regard, all the Defendants have engaged in a related series of transactions to engage in unlawful reproduction and distribution of Plaintiff's copyrighted Motion Picture. Each Defendant traded the exact same file.

23. Each of the Defendant's acts of infringement have been willful, intentional, and in disregard of and with indifference to the rights of Plaintiff. The technology used to identify each Defendant is explained in **Exhibit B**.

24. Plaintiff has suffered both money damages and irreparable harm as a result of each Defendant's infringement of Plaintiff's copyrights in the Motion Picture. In addition,

discovery may disclose that one or more of the Defendants obtained profits as a result of such infringement.

25. As a result of each Defendant's infringement of Plaintiff's exclusive rights under copyright, Plaintiff is entitled to monetary relief pursuant to 17 U.S.C. § 504, which may include Plaintiff's damages caused by each Defendant and each Defendant's profits and/or statutory damages, and to Plaintiff's attorney fees and costs pursuant to 17 U.S.C. § 505.

26. The conduct of each Defendant has caused, is causing and, unless enjoined and restrained by this Court will continue to cause, Plaintiff great and irreparable injury that cannot fully be compensated or measured in money. Plaintiff has no adequate remedy at law. Pursuant to 17 U.S.C. §§ 502 and 503, the Plaintiff is entitled to injunctive relief prohibiting each Defendant from further infringing Plaintiff's copyrights and ordering that each Defendant destroy all copies of the copyrighted motion pictures made in violation of the Plaintiffs' copyrights.

## **COUNT II**

### **CONTRIBUTORY INFRINGEMENT**

27. Plaintiff repeats and reincorporates herein the allegations set forth in paragraphs 1-26, above.

28. Plaintiff is, and at all relevant times has been, the owner of the copyrights and/or the owner of the exclusive rights under the copyrights in the United States in the Motion Picture at issue.

29. Through use of torrent software and the process described above, each Defendant copied the constituent elements of the copyrighted work. Further, each Defendant traded not just the same copyrighted work, but the exact same file, as shown by the identical hash value.

30. By participating in the file swapping with the other Defendants, each Defendant induced or caused or materially contributed to the infringing conduct of the other Defendants.

31. Each Defendant knew or should have known that other torrent users (Defendants) involved in the file swapping were infringing upon Plaintiff's copyrighted work. Each Defendant directly participated in the series of uploading and downloading of the exact same file and therefore materially contributed to each other Defendant's infringing activities.

32. Each of the Defendants' contributory infringements were committed willfully within the meaning of 17 U.S.C. § 504(c)(2).

33. As a result, Plaintiff has suffered damages that were proximately caused by each of the Defendants. Plaintiff has suffered both money damages and irreparable harm as a result of each Defendant's infringement of Plaintiff's copyrights in the Motion Picture. In addition, discovery may disclose that one or more of the Defendants obtained profits as a result of such infringement.

34. The conduct of each Defendant has caused, is causing and, unless enjoined and restrained by this Court will continue to cause, Plaintiff great and irreparable injury that cannot fully be compensated or measured in money. Plaintiff has no adequate remedy at law. Pursuant to 17 U.S.C. §§ 502 and 503, the Plaintiff is entitled to injunctive relief prohibiting each Defendant from further infringing Plaintiff's copyrights and ordering that each Defendant destroy all copies of the copyrighted motion pictures made in violation of the Plaintiffs' copyrights.

### **RELIEF REQUESTED**

WHEREFORE, Plaintiff requests that the Court enter judgment against each Defendant as follows:

A. For a judgment that such Defendant has infringed Plaintiff's copyright in the Motion Picture;

B. For entry of preliminary and permanent injunctions providing that such Defendant shall be enjoined from directly or indirectly infringing the Plaintiffs' rights in the Motion Picture, including without limitation by using the Internet to reproduce or copy the Motion Picture, to distribute the Motion Picture, or to make the Motion Picture available for distribution to anyone, except pursuant to a lawful license or with the express authority of Plaintiffs;

C. For entry of preliminary and permanent mandatory injunctions providing that such Defendant shall destroy all copies of the Motion Picture that Defendant has downloaded onto any computer hard drive or server without Plaintiff's authorization and shall destroy all copies of the Motion Picture transferred onto any physical medium or device in Defendant's possession, custody, or control;

D. For entry of judgment that such Defendant shall pay actual damages and profits, or statutory damages, pursuant to 17 U.S.C. § 504, at the election of Plaintiff;

E. For entry of judgment that such Defendant shall pay Plaintiff's costs;

F. For entry of judgment that such Defendant shall pay Plaintiff's reasonable attorney fees; and

G. For entry of judgment that Plaintiff have such other relief as justice may require and/or as otherwise deemed just and proper by this Court.

Respectfully submitted this 8th day of May, 2012.

FOR THE PLAINTIFF:

By:     /s/ Mike Meier      
Mike Meier (NY9295)  
The Copyright Law Group, PLLC  
4000 Legato Road, Suite 1100  
Fairfax, VA 22033  
Phone: (888) 407-6770  
Fax: (703) 546-4990  
Email:  
mike.meier.esq@copyrightdefenselawyer.com

ATTORNEY FOR PLAINTIFF

### VERIFICATION

I, Mike Meier, am the attorney who prepared this Complaint. I verify and declare under 28 USC § 1746 that I have read the foregoing Complaint and it is, based on my personal knowledge and information I have reviewed, true. In particular, I have taken the following steps to ensure that the Complaint and its allegations comply with all requirements:

- 1) I have personally discussed in detail the data about alleged infringers (identified by IP address) with a technical specialist at the Copyright Enforcement Group (CEG), Mr. Jon Nicolini, Vice President of Technology. Mr. Jon Nicolini explained the commonality of all identified IP addresses: (a) The devices connected to all IP addresses identified have utilized the same exact hash mark (a 40-character hexadecimal string which through cryptographic methods clearly identifies the Release - comparable to a fingerprint) which corroborates them within the same series of transactions; (b) all alleged infringers downloaded the same file of the copyrighted work while trading in the same torrent; (c) Mr. Jon Nicolini also explained that he made an effort to create a list of alleged infringers who are located within the jurisdiction of the court where the Complaint is to be filed by using geo-location technology; (d) Mr. Jon Nicolini specifically limited the time period during which the investigated alleged downloads occurred to ensure commonality amongst the alleged infringers. Thus the alleged infringers were likely within the same swarm and engaged in a series of related transactions. The identified IP addresses shared the files around the same time. Mr. Jon Nicolini explained that the alleged infringers so identified downloaded the identical file of the copyrighted work as part of the same series of transactions or occurrences, and are thus related.
- 2) I particularly inquired into the issue of the relationship among the alleged infringers by (i) researching the functioning of torrent technology, (ii) participating in live demonstrations of torrent software, and (iii) interviewing CEG personnel. Mr. Jon Nicolini explained that the alleged infringers in this case engaged in a series of related transactions, because they all downloaded the exact same file (not just the same copyrighted work), within a limited period of time. Furthermore, because of the nature of torrent software, they engaged in a series of related transactions because in order to download a movie (or parts of it), one must permit other users to download and/or upload the file from one's own computer. Thus, the Defendants were simultaneously trading (downloading and/or uploading) the exact same file during a limited period of time. While Defendants engaged in this downloading and/or uploading of the file, they exposed their IP address. With torrent software, one can see the IP address of the various computers that they are connected to, and which are sharing files in cooperation with, one's own computer.
- 3) Mr. Jon Nicolini further confirmed to me the direct digital connection and relationship among the infringers based on the torrent process and provided the following additional information: The process begins with one user accessing the Internet through an Internet Service Provider ("ISP") and intentionally making a digital file of the work available on the Internet to the public from his or her



computer. This first file is often referred to as the first "seed." The person making this seed available as the "original seeder." Persons seeking to download such a work also access the Internet through an ISP (which may or may not be the same ISP as used by the original seeder) and seek out the work on a P2P network. With the availability of the seed, other users, who are referred to as "peers," access the Internet and request the file (by searching for its title or even searching for the torrent's "hash") and engage the original seeder and/or each other in a group, sometimes referred to as a "swarm," and begin downloading the seed file. In turn, as each peer receives portions of the seed, most often that peer makes those portions available to other peers in the swarm. Therefore, each peer in the swarm is at least copying and is usually distributing, as a follow-on seeder, copyrighted material at the same time. Any BitTorrent client may be used to join a swarm. As more peers join a swarm at any one instant, they obtain the content at even greater speeds because of the increasing number of peers simultaneously offering the content as seeders themselves for unlawful distribution. As time goes on, the size of the swarm varies, yet it may endure for a long period, with some swarms enduring for 6 months to well over a year depending on the popularity of a particular motion picture. That is, each peer (i.e. member of a swarm) in a P2P network has acted and acts in cooperation with the other peers by agreeing to provide, and actually providing, an infringing reproduction of at least a substantial portion of a copyrighted work in anticipation of the other peers doing likewise with respect to that work and/or other works. Joining a P2P network is an intentional act, requiring the selection by a peer of multiple links to do so.

- 4) I also inquired into the issue of jurisdiction over the alleged infringers. Mr. Jon Nicolini and other CEG personnel explained that they make every effort to ensure that all alleged infringers have in fact engaged in a series of related transactions and can thus be properly joined in one lawsuit. Most importantly: (i) CEG has identified only alleged infringers who traded exactly the same file of the copyrighted works at issue (not just the same copyrighted work), as identified by the hash value; and (ii) CEG has limited the time period during which they searched copyright infringements; in addition, (iii) CEG has limited the geographic search to ensure as much as technically possible that the alleged infringers are in fact within the geographic area of the court. However, because of intermediary ISPs and the location of the ISPs technical facilities, the location cannot always be exactly pinpointed.
- 5) I personally conducted a random batch test of the purported locations of the IP addresses in Exhibit A to ensure that the Defendants likely reside within the jurisdiction of the Court or can be found there, or a substantial part of the events alleged occurred or had an effect within the jurisdiction of the Court. I checked the locations through the IP locators at <http://www.ip-address.org> and/or <http://www.arin.net> and/or <http://www.ipligence.com>. During my search, I did not find any IP addresses that were outside the geographic area of the Court. However, I know that such location checks are not absolutely accurate in all circumstances. For example, because my personal checks were conducted after the file swapping took place, the IP address may have changed. However, I have used my best efforts to ensure that all Defendants are in fact residents of the State and/or within the geographic location of the Court.

- 6) I have personally participated in two training sessions on torrent software, conducted by Copyright Enforcement Group technical personnel, including a live demonstration of the use of torrent software. I personally saw the multiple steps that are required to log into a torrent system to trade files with one another, that each user must connect with other users and simultaneously upload and download (“trade”) a particular file for the file swapping to work, and that the users’ IP addresses are exposed during the process so that one can see who is simultaneously uploading and downloading the file from one’s own computer.
- 7) I personally checked that a copyright registration for the work at issue has been filed properly through the searchable database of the U.S. Copyright office at <http://copyright.gov/records/>, to ensure that the work at issue is eligible for statutory remedies under Section 412 of the Copyright Law.

Thus, I verify and declare under penalty of perjury that the foregoing statements and the statements in the Complaint are true and correct to the best of my knowledge.

Date: May 8, 2012

/s/ Mike Meier  
Mike Meier

**EXHIBITS:**

Exhibit A – Table of Last-Observed Infringements by Defendants of Plaintiff's Copyright in the Motion Picture.

Exhibit B – Technology Declaration of Mr. Jon Nicolini, explaining the technology used to identify the alleged copyright infringers.

Exhibit C – Copyright registration record of the Motion Picture at issue.

Exhibit D – Believed State of Residence for each John Doe

**Exhibit A – Table of Last-Observed  
Infringements by Defendants of Plaintiff's  
Copyright in the Motion Picture.**

## Exhibit A

Table of Last-Observed Infringements by Defendants of Digital Sin Inc's Copyright in the Motion Picture [REDACTED] Copyright Reg. No. in process. Copyright Application Service Request No. 1-714915653 filed on 2012-01-23.

Defendant	Internet Protocol Address (IP)	Timestamp (U.S. Eastern Time)	Internet Service Provider (ISP)	Protocol	Hash
Doe 1	108.21.193.169	2012-02-20 22:11:18 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 2	108.41.125.66	2012-03-03 23:06:09 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 3	108.41.147.9	2012-02-26 00:01:28 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 4	108.41.152.140	2012-02-04 14:49:16 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 5	108.41.46.76	2012-02-08 23:11:03 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 6	108.6.23.211	2012-02-18 11:08:00 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 7	173.52.212.130	2012-02-13 23:08:51 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 8	173.62.31.10	2012-03-11 17:09:20 -0400	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 9	173.62.36.144	2012-02-06 17:05:43 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 10	66.108.63.72	2012-02-05 04:59:19 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 11	68.174.63.239	2012-02-19 04:47:31 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 12	68.175.76.231	2012-02-05 23:04:25 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 13	69.22.232.160	2012-02-07 12:49:17 -0500	EarthLink	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 14	69.86.35.49	2012-02-10 22:57:33 -0500	EarthLink	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 15	71.169.48.8	2012-02-20 14:17:04 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 16	71.183.204.59	2012-03-08 00:03:04 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 17	74.101.43.93	2012-03-04 23:12:22 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 18	74.68.152.213	2012-03-25 05:14:57 -0400	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 19	74.73.146.236	2012-03-03 11:08:58 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 20	74.73.170.83	2012-02-27 23:15:54 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 21	96.246.225.104	2012-02-03 11:09:17 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 22	98.14.190.209	2012-03-04 19:48:45 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 23	98.15.154.106	2012-02-19 16:12:23 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 24	98.15.188.109	2012-02-17 23:05:46 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 25	98.15.188.189	2012-02-17 17:11:01 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 26	98.15.194.177	2012-03-16 10:57:10 -0400	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 27	98.15.250.29	2012-03-10 11:11:11 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4



Exhibit B – Technology Declaration of Mr. Jon Nicolini, explaining the technology used to identify the alleged copyright infringers

## Exhibit C – Copyright registration record of the Motion Picture at issue



\*-APPLICATION-\*

Title \_\_\_\_\_

**Title of Work:** [REDACTED]

Completion/Publication \_\_\_\_\_

**Year of Completion:** 2012

**Date of 1st Publication:** January 19, 2012

**Nation of 1st Publication:** United States

Author \_\_\_\_\_

▪ **Author:** Digital Sin Inc

**Author Created:** entire motion picture

**Work made for hire:** Yes

**Citizen of:** not known

**Domiciled in:** not known

**Anonymous:** Yes

Copyright claimant \_\_\_\_\_

**Copyright Claimant:** Digital Sin Inc

21345 Lassen Street, Chatsworth, CA, 91311

Certification \_\_\_\_\_

**Name:** Sonia Bang

**Date:** January 23, 2012

**Registration #:**

**Service Request #:** 1-714915653

**Priority:** Routine

**Application Date:** January 23, 2012 05:47:11 PM

Correspondent \_\_\_\_\_

**Organization Name:** Digital Sin Inc

**Name:** Sonia Bang

**Email:** soniab@newsensations.com

**Telephone:** 818-773-4999

**Address:** 21345 Lassen Street  
Chatsworth, CA 91311

Mail Certificate \_\_\_\_\_

Digital Sin Inc  
Sonia Bang  
21345 Lassen Street  
Chatsworth, CA 91311

## Exhibit D – Believed State of Residence for each John Doe

## Exhibit A

Table of Last-Observed Infringements by Defendants of Digital Sin Inc's Copyright in the Motion Picture [REDACTED] Copyright Reg. No. in process. Copyright Application Service Request No. 1-714915653 filed on 2012-01-23.

Defendant	Internet Protocol Address (IP)	Timestamp (U.S. Eastern Time)	Internet Service Provider (ISP)	Protocol	Hash
Doe 1	108.21.193.169	2012-02-20 22:11:18 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 2	108.41.125.66	2012-03-03 23:06:09 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 3	108.41.147.9	2012-02-26 00:01:28 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 4	108.41.152.140	2012-02-04 14:49:16 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 5	108.41.46.76	2012-02-08 23:11:03 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 6	108.6.23.211	2012-02-18 11:08:00 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 7	173.52.212.130	2012-02-13 23:08:51 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 8	173.62.31.10	2012-03-11 17:09:20 -0400	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 9	173.62.36.144	2012-02-06 17:05:43 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 10	66.108.63.72	2012-02-05 04:59:19 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 11	68.174.63.239	2012-02-19 04:47:31 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 12	68.175.76.231	2012-02-05 23:04:25 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 13	69.22.232.160	2012-02-07 12:49:17 -0500	EarthLink	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 14	69.86.35.49	2012-02-10 22:57:33 -0500	EarthLink	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 15	71.169.48.8	2012-02-20 14:17:04 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 16	71.183.204.59	2012-03-08 00:03:04 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 17	74.101.43.93	2012-03-04 23:12:22 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 18	74.68.152.213	2012-03-25 05:14:57 -0400	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 19	74.73.146.236	2012-03-03 11:08:58 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 20	74.73.170.83	2012-02-27 23:15:54 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 21	96.246.225.104	2012-02-03 11:09:17 -0500	Verizon Internet Services	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 22	98.14.190.209	2012-03-04 19:48:45 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 23	98.15.154.106	2012-02-19 16:12:23 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 24	98.15.188.109	2012-02-17 23:05:46 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 25	98.15.188.189	2012-02-17 17:11:01 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 26	98.15.194.177	2012-03-16 10:57:10 -0400	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4
Doe 27	98.15.250.29	2012-03-10 11:11:11 -0500	Road Runner	BitTorrent	7208828099f0edeb9c4f016b86f355ddfb786ed4



UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

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

Plaintiff,

-v-

DOES 1-27,

Defendants.  
-----X

**USDC SDNY**  
**DOCUMENT**  
**ELECTRONICALLY FILED**  
DOC #:  
DATE FILED: 6/6/2012

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



**July 31, 2012**

**READ AT ONCE**

**COURT-DIRECTED NOTICE  
REGARDING ISSUANCE OF SUBPOENA  
SEEKING DISCLOSURE OF YOUR IDENTITY**

Verizon Online, as your Internet Service Provider, recently received a legal document called a subpoena. Absent action by you, the subpoena requires us to disclose your name, address and other information. The subpoena was issued pursuant to a Court Order in a lawsuit pending in the United States District Court for the Southern District of New York.

The Plaintiffs have filed a lawsuit alleging that various people have perhaps infringed their copyrights by illegally downloading and/or distributing a movie. However, the Plaintiffs do not know the actual names or addresses of these people – only the Internet Protocol address (“IP address”) of the computer associated with the allegedly illegal activity.

Accordingly, Plaintiffs have filed lawsuits against so-called anonymous “John Doe” defendants and issued subpoenas to determine the identity of these people (the so-called “John Does”). The Plaintiffs have asked us to disclose your identification information to them, including your name, current (and permanent) addresses, and your email address and Media Access Control number. Enclosed is a copy of the subpoena seeking your information and the exhibit page containing the IP address that has been associated with your computer and showing the date and time you are alleged to have used the Internet to download or upload the particular movie. (The plaintiffs will have to prove that you illegally used the internet to download or upload the particular movie. We do not have records that would prove or disprove that fact; we simply have records that show that an IP address was assigned to a specific customer at a specific time. It may be that someone else, for a variety of reasons, was using the IP address).

This is a civil lawsuit, not a criminal case. You have not been charged with any crime. If the Plaintiffs receive your information from your Internet Service Provider, you will likely be added as a named defendant to their lawsuit.

**INFORMATION ABOUT YOU HAS NOT YET BEEN DISCLOSED,  
BUT IT WILL BE DISCLOSED IN 30 DAYS IF YOU DO NOT  
CHALLENGE THE SUBPOENA.**

Your identifying information has not yet been disclosed to the Plaintiffs.

This notice is intended to inform you of some of your rights and options. It does not provide legal advice. We cannot advise you about what grounds exist, if any, to challenge this subpoena. If you would like legal advice you should consult an attorney. Within this notice you

will find a list of resources that may help you locate an attorney and decide how to respond to the subpoena or lawsuit

If you want to prevent being identified, you have 30 days from the date of this notice to file a motion to quash or vacate the subpoena and notify Verizon Online that you have done so. You must also notify your ISP. If you need more than 30 days to file such a motion or find a lawyer to assist you, you can file a motion asking for an extension of time; you should notify Verizon Online if you file a motion asking for more time. The appropriate address to send such notices to Verizon is:

Verizon Legal Compliance  
Custodian of Records  
P.O. Box 1001  
San Angelo, TX 76902

*Fax Number: 325-949-6916*

Please provide us with a copy of the filed motion to quash the subpoena, your identity will not be disclosed until the court makes a decision on your motion. If you do nothing, then after 30 days we are compelled to send the Plaintiff your name, address, email address, telephone number, and your modem's Media Access Control number.

You may wish to obtain an attorney to advise you on these issues or to help you take action.

To help you find a lawyer, the American Bar Association's attorney locator can be found on the Internet at <http://www.abanet.org/lawyerlocator/searchlawyer.html>

The Electronic Frontier Foundation is an organization that seeks to protect the rights of Internet users. They have created a website that lists attorneys who have volunteered to consult with people in your situation and contains further information about the lawsuit that has been filed against you as well as similar lawsuits:

<https://www.eff.org/issues/file-sharing/subpoena-defense>

If you are interested in discussing this matter with the Plaintiff's attorneys, you may contact them by telephone at 888-407-6770. But please understand that these lawyers represent the company that is trying to sue you. They can speak with you about settling the lawsuit, if you wish to consider that. At the same time, you must be aware that if you contact them they may learn your identity, and that anything you say to them can later be used against you in court.

You should not call the Court.

Again, you may wish to retain an attorney to discuss these issues and your options.

**REDACTED**

108.21.193.169 2/21/2012 3:11:18 AM GMT



AO 88D (Rev. 06/09) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

UNITED STATES DISTRICT COURT

for the  
Northern District of Texas

Digital Sin, Inc.	)	
<i>Plaintiff</i>	)	
v.	)	Civil Action No. 12-CV-03873-JMF
DOES 1-27	)	
<i>Defendant</i>	)	(If the action is pending in another district, state where: Southern District of New York )

**SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS  
OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION**

To: Custodian of Records, Verizon Internet Services (hereinafter "ISP"), Legal Compliance  
P.O. Box 1001, TXD01613, San Angelo, TX 76902

**Production:** YOU ARE COMMANDED to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and permit their inspection, copying, testing, or sampling of the material:

Documents sufficient to identify the names, addresses, email addresses, and any other court-ordered information as set forth in the Order attached hereto as Attachment B of ISP's subscribers assigned the IP addresses identified on Attachment A on the corresponding dates at the corresponding times. You are to comply with this subpoena pursuant to the terms set forth in the Order attached hereto as Attachment B.

Place: Westwood RL Attn: Westwood Network - Mike Meier 6923 Indiana Avenue, 274 Lubbock, TX 79413	Date and Time: August 11, 2012 at 9:00 a.m.
--	--

**Inspection of Premises:** YOU ARE COMMANDED to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:
--------	----------------

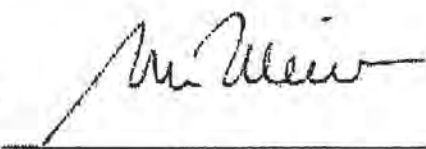
The provisions of Fed. R. Civ. P. 45(c), relating to your protection as a person subject to a subpoena, and Rule 45 (d) and (e), relating to your duty to respond to this subpoena and the potential consequences of not doing so, are attached.

Date: June 12, 2012

CLERK OF COURT

OR

\_\_\_\_\_  
*Signature of Clerk or Deputy Clerk*

  
\_\_\_\_\_  
*Attorney's signature*

The name, address, e-mail, and telephone number of the attorney representing (name of party) Digital Sin, Inc., who issues or requests this subpoena, are:  
Mike Meier, The Copyright Law Group, PLLC, 4000 Legato Road, Suite 1100, Fairfax, VA 22033, Email: contact@copyrightdefenselawyer.com, Telephone: 888-407-6770

## ATTACHMENT A

Table of Observed Infringements by Defendants of Digital Sin, Inc.'s Copyright Reg. No. PA0001780990

Defendant	Internet Protocol Address (IP) / Timestamp (U.S. Eastern Time)	Internet Service Provider (ISP)	State / District Court	Protocol / Hash
Doe 1	108.21.193.169 / 2012-02-20 22:11:18 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 2	108.41.125.66 / 2012-03-03 23:06:09 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 3	108.41.147.9 / 2012-02-26 00:01:28 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 4	108.41.152.140 / 2012-02-04 14:49:16 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 5	108.41.46.76 / 2012-02-08 23:11:03 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 6	108.6.23.211 / 2012-02-18 11:08:00 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 7	173.52.212.130 / 2012-02-13 23:08:51 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 8	173.62.31.10 / 2012-03-11 17:09:20 -0400	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 9	173.62.36.144 / 2012-02-06 17:05:43 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 15	71.169.48.8 / 2012-02-20 14:17:04 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 16	71.183.204.59 / 2012-03-08 00:03:04 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 17	74.101.43.93 / 2012-03-04 23:12:22 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4
Doe 21	96.246.225.104 / 2012-02-03 11:09:17 -0500	Verizon Internet Services	New York / Southern District of New York	BitTorrent / 7208828099f0edeb9c4f 016b86f355ddfb786ed4

**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.

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

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

Plaintiff,

-v-

DOES 1-27,

Defendants.  
-----X

**USDC SDNY**  
**DOCUMENT**  
**ELECTRONICALLY FILED**  
DOC #:  
DATE FILED: 6/6/2012

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