UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

DIGITAL SIN, INC. 21345 Lassen St. Chatsworth, CA 91311 Plaintiff, v. DOES 1 – 176 Defendants.	)	Civil Action 1:12-cv-00126-AJN

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

Plaintiff filed a Complaint against John Does who have traded the same exact file of Plaintiff's copyrighted work without authorization through a file-swapping network ("Peer-to-Peer" or "P2P" network). All John Does are believed to reside in New York.

Plaintiff can obtain the Defendants' names and addresses only from the non-party Internet Service Providers ("ISPs") that provide internet services to the Doe defendants. The ISPs have such information readily available and keep it in the regular course of business.

Pursuant to Fed. R. Civ. P. 26(b)(1) and (d)(1), Plaintiff moves for entry of an Order granting it leave to serve third party subpoenas prior to a Rule 26(f) conference ("Motion"), and submits the following Memorandum in support. Attached is the *Declaration of Jon Nicolini* in Support of Plaintiff's Motion For Leave to Take Discovery Prior to a Rule 26(f) Conference ("Nicolini Declaration") to corroborate the statements in this Memorandum.

This Memorandum also addresses the issues of Joinder and Personal Jurisdiction. Please note that Joinder and Personal Jurisdiction were addressed in the Complaint, as well as in the *Declaration of Jon Nicolini* that was attached to the Complaint. As for Joinder, the Complaint and the Declaration of Jon Nicolini explain that the Doe defendants engaged in a related series of transactions because they all intentionally distributed exactly the same file (as shown by the hash mark). *See further explanations, below*.

As for Jurisdiction, as alleged in the Complaint and the *Declaration of Jon Nicolini*, Plaintiff has made efforts to ensure that all Doe defendants are in fact located in New York. Each Doe defendant is believed to reside in New York. *See Exhibit D to the Complaint*.

I. INTRODUCTION

Plaintiff is seeking leave of Court to serve a Rule 45 subpoena upon Defendants' ISPs and any related intermediary ISPs. Any such subpoena will demand the true name, address, e-mail address and Media Access Control ("MAC") address of the Defendant to whom the ISP issued an IP address. Plaintiff is *not* seeking telephone numbers.

Courts have routinely permitted discovery to identify "Doe" defendants. *See Warner Bros. Records, Inc. v. Does 1-6*, 527 F.Supp.2d 1, 2 (D.D.C. 2007) (Rule 45 subpoena upon Georgetown University to obtain the true identity of each Doe defendant) (citing Memorandum Opinion and Order, *UMG Recordings, Inc. v. Does 1-199*, No. 04-093(CKK) (D.D.C. March 10, 2004)); *Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1 (D.D.C. 2008).

Because Defendants used internet-based file-swapping networks to commit the infringements, Plaintiff only knows the Defendants by their Internet Protocol ("IP") addresses. Defendants' IP addresses were assigned to the Defendants by their respective Internet Service Providers (ISPs). Both the IP addresses and ISPs are set forth in Exhibit A to the Complaint. The

ISPs can identify the Defendants through the IP addresses. The ISPs maintain internal information logs that record the date, time and customer identity for each IP address. The ISPs, however, usually maintain these information logs for only a short period of time.

II. JURISDICTION

In two recent cases, the Southern District of New York has raised the issue of jurisdiction in copyright infringement cases. *See Digiprotect USA Corp. v. John/Jane Does 1-266*, 10 Civ. 8759 (TPG) (April 13, 2011) ("Digiprotect I") & *Digiprotect USA Corp. v. John/Jane Does 1-240* (PAC) (September 26, 2011) ("Digiprotect II"). In those cases, the Plaintiff lumped Doe defendants from different parts of the U.S. together. In *Digiprotect I*, Plaintiff alleged that its injury had occurred in New York and because of the nature of peer-to-peer file sharing, New York residents were likely involved. Only 20 to 25 of the 266 IP addresses were located in New York. In *Digiprotect II*, only 10 of the 240 IP addresses were located in New York, and Plaintiff Digiprotect argued that there is jurisdiction if any one Doe resides in New York. *See Digiprotect II*, slip op. at 5.

Unlike the *Digiprotect* cases, all Doe defendants in the present case reside in New York, and jurisdiction is thus proper. *N.Y. C.P.L.R. Section 301 (general jurisdiction requires that the defendant reside, do business, or be served with process while in New York)*. Plaintiff has made a *prima facie* showing of jurisdiction over the Doe defendants. *See attached Declaration of Jon Nicolini, as well as Exhibit D to the Complaint*.

The Declaration of Jon Nicolini, attached to the Complaint, stated:

> 18. Users subscribe to the services of an ISP to gain access to the Internet. Each time a subscriber accesses the Internet, the ISP provides a unique Internet Protocol ("IP") address to the subscriber. … Taking advantage of this technology and the unique metadata associated with the file containing unlawful copy of CEG's client's motion picture, CEG's System inspects file-

sharing networks for computers that are distributing at least a substantial portion of a copy of a copyrighted work owned by Plaintiff, and when CEG finds such a computer, CEG's System also collects the following publicly accessible information: (a) the time and date the infringer was found, (b) the time(s) and date(s) … *In addition, CEG uses available databases to record the name of the ISP having control of the IP address and the state (and often the city or county) associated with that IP address.* …

19. … *If one knows a computer's Internet Protocol address, one can, using publicly available reverse-lookup databases on the Internet, identify the ISP used by that computer and the city (or county) and state in which the computer was located at the date and time that the Internet Protocol address was obtained*. … […]

25. We have made 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) We have identified only alleged infringers who traded exactly the same file of the copyrighted works at issue (not just the same copyrighted work); and (ii) we have limited the time period during which we searched copyright infringements; in addition, (iii) *we have 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.* ….

Declaration of Jon Nicolini, paras. 18-25 (*italics added*).

In sum, this Court has jurisdiction over the Doe defendants because based on the information available, the internet connections of all Does (and thus in all likelihood also their residences) are in New York.

III. JOINDER

Pursuant to Fed.R.Civ.P. 20(a)(2), the Defendants have been properly joined, as set forth in detail below and in the supporting *Declaration of Jon Nicolini*, because Plaintiff alleges that all Defendants have intentionally traded (uploaded and downloaded) the exact same file of the copyrighted works in related transactions through torrent software.

Unlike the *Digiprotect* cases, where the Doe defendants had allegedly committed the same type of offense by file sharing and distributing the same movie, the Doe defendants in this case shared and distributed not just the same movie, but *exactly the same file as identified by the hash mark*. Unlike the list of Doe defendants in the *Digiprotect* cases, the case at bar included a

list of Doe Defendants showing the identical hash mark for the shared file. *Compare List of Doe Defendants in the Digiprotect cases to the List of Doe Defendants (Exhibit A) in the present case.*

The Doe 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 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:*

5. Therefore, the original seeder and each of the members of the swarm (i.e., each peer) must have separately installed on their respective computers special software that allows peer-to-peer sharing of files by way of the Internet. The most popular type of peer-to-peer file sharing program utilizes the BitTorrent protocol. …. In any event, *the seeder and each member of the swarm (i.e., peer) must intentionally install a BitTorrent client* (i.e., software application) onto his or her computer before that computer can be used to join a BitTorrent file sharing network.

6. P2P networks distribute infringing copies of motion pictures (and works in other forms such as music and books) with file sharing software such as BitTorrent as follows: *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."

7. …. 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.*

Declaration of Jon Nicolini, paras. 5-7 (*italics added*).

Therefore, the Doe defendants are properly joined.

IV. ARGUMENT

Plaintiff needs the identity of the Doe Defendants to prosecute the claims made in its Complaint. Without this information, Plaintiff cannot serve the Defendants, and will be unable to pursue this lawsuit to protect its copyrights.

Pursuant to Rule 26(b)(1) and (b)(1), courts may issue an Order permitting discovery prior to a Rule 26(f) conference "[f]or good cause" and for "any matter relevant to the subject matter involved in the action."

In copyright infringement cases, courts routinely find good cause exists to issue a Rule 45 subpoena to discover a Doe defendant's identity prior to a Rule 26(f) conference where a plaintiff makes: (1) a prima facie showing of infringement, (2) there is no other way to identify the Doe Defendant, and (3) there is a risk an ISP will destroy its logs prior to the conference. *See Patrick Collins, Inc. v. John Does 1 – 21,* Civil Action No. 1:11-cv-05784 (S.D.N.Y., Order of September 22, 2011)*; UMG Recording, Inc. v. Doe*, 2008 WL 4104214, *4 (N.D. Cal. 2008); *Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 6-7 (D.D.C. 2008) (noting the overwhelming number of cases where copyright infringement plaintiffs sought to identify Doe defendants and courts routinely applied the good cause standard to permit discovery).

Here, good cause exists to grant the Order.

A. Courts Permit Discovery to Identify John Doe Defendants

Courts have uniformly approved the procedure of suing John Doe defendants and then using discovery to identify such defendants. In fact, federal district courts, including this Court, have granted such expedited discovery in "Doe" defendant actions that are factually similar or identical to the case at bar. These cases include *Patrick Collins, Inc. v. John Does 1 – 21,* Civil

Action No. 1:11-cv-05784 (S.D.N.Y., Order of September 22, 2011); *Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 7 (D.D.C. Apr. 28, 2008) (Kollar-Kotelly, J.); *Patrick Collins, Inc. v. Does 1 – 14*, No. 8:11-cv-01773-AW (Md., Order of August 2, 2011); *Metro-Goldwyn-Mayer Pictures Inc., et al. v. Does 1-10*, Case No. 04-2005 (JR) (D.D.C.) (Robertson, J.); *Twentieth Century Fox Film Corporation, et al. v. Does 1-9*, Case No. 04-2006 (EGS) (D.D.C.) (Sullivan, J.); Lions Gate Films, Inc., et al. v. Does 1-5, Case No. 05-386 (EGS) (D.D.C.) (Sullivan, J.); *UMG Recordings, et al. v. Does 1-199*, Case No. 04-093 (CKK) (D.D.C.) (Kollar-Kotelly, J.); *Caroline Records, Inc., et al. v. Does 1-175*, Case No. 04 2028 (D.D.C.) (Lamberth, J.).

In such cases, copyright holder plaintiffs obtained the identities of the file-swapping network users from ISPs through expedited discovery based on information similar to the information provided in Exhibit A to the Complaint (identification of alleged infringers through IP address and ISP).

B. Good Cause Exists to Grant the Motion

1. Plaintiff Properly Pled Copyright Infringement

Plaintiff has properly pled a cause of action for copyright infringement:

8. The Motion Picture "My Little Panties #2" (the "Motion Picture") was produced by Plaintiff and released on November 4, 2010. The copyright was registered on February 10, 2011, the Copyright Registration Number is PA0001733587 / 2011-02-10. **See Exhibit C.** It is offered as a DVD through various vendors, including www.cduniverse.com for $22.49, and as "video on demand."

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.

11. In this case, all Defendants have not only swapped the same copyrighted work, they have swapped 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.

Complaint at paras. 8-13.

Further, Plaintiff's allegations of infringement by the particular Doe Defendants are confirmed by an affidavit from a technical specialist employed by the company that investigated the infringements, Jon Nicolini. *See attached Declaration of Jon Nicolini ("Nicolini Declaration"), paras. 11-22*:

11. CEG utilizes a system of software components ("the System") conceptualized, developed, and maintained by me in order to collect data about unauthorized distribution of copies of copyrighted works on P2P networks. […]

16. In this case, the P2P network on which we found unauthorized distribution of Plaintiff's Work was a BitTorrent network. […]

18. […] Taking advantage of this technology and the unique metadata associated with the file containing unlawful copy of CEG's client's motion picture, CEG's System inspects file-sharing networks for computers that are distributing at least a substantial portion of a copy of a copyrighted work owned by Plaintiff, and when CEG finds such a computer, CEG's System also collects the following publicly accessible information: (a) the time and date the infringer was found, (b) the time(s) and date(s) when a portion of the accused file was downloaded successfully to the accused infringer's computer, (c) the time and date the infringer was last successfully connected to via the P2P network with respect to the infringer's computer's

downloading and/or uploading the accused file to the Internet (hereinafter referred to as "Timestamp"), (d) the IP address assigned to the infringer's computer, (e) the P2P software application used by the infringer and the port number used by the infringer's P2P software, (f) the size of the accused file, and that file's MD5 checksum, and SHA-1 checksum (the last of which is the unique "hash" referred to above), (g) the percent of the file downloaded by us from the infringer's computer, (h) the percent of the accused file on the infringer's computer which is available at that moment for copying by other peers, and (i) any relevant transfer errors. […] CEG has confirmed that each of the files obtained from the Defendants that are listed in **Exhibit A** attached to the Complaint filed in this case is a copy of a substantial portion of the copyrighted work listed in **Exhibit A**. All of this information is stored in database files on CEG's computers. […]

Accordingly, Plaintiff has pled a prima facie case.

2. Plaintiff has no other Way of Identifying the Doe Defendants

Plaintiff can obtain the identities of the Doe Defendants only from the ISPs:

19. […] If one knows a computer's Internet Protocol address, one can, using publicly available reverse-lookup databases on the Internet, identify the ISP used by that computer and the city (or county) and state in which the computer was located at the date and time that the Internet Protocol address was obtained. However, the actual name and address of the person subscribing to the ISP's service is neither publicly available, nor available to CEG.

20. However, with the Internet Protocol address and the date and time that the infringer's computer was accessing the Internet through the ISP, the ISP (be it AT&T, Verizon, Qwest, Comcast or any of many other ISPs) can review its own subscriber logs to identify either (i) the names and addresses of the subscriber, or (ii) the intermediary ISP through which the person is ultimately subscribed to the main ISP. *Nicolini Declaration, paras. 19-20.*

Other than obtaining this information from the ISPs, there is no other way of determining the Defendants' true identities. Since there is no other way for Plaintiff to obtain Defendants' identities, except by serving a subpoena on Defendants' ISPs, there is good cause to grant the Motion.

Also, it is not possible for the Plaintiff to have a 26(f) conference with the Defendants until Plaintiff knows their identities and can serve them.

3. There is a Risk that an ISP will Destroy its Information Logs

Prior to a Rule 26(f) Conference

Unaware of the present lawsuit, the ISPs at issue will likely destroy the information logs in the normal course of business and Plaintiff's right to sue Defendants for copyright infringement may be forever lost. ISPs retain this type of information usually for only a few months. *See UMG Recordings, Inc. v. Doe, 2008 WL 4104214 (N.D. Cal. 2008) (finding good cause for expedited discovery exists in Internet infringement cases, where a plaintiff makes a prima facie showing of infringement, there is no other way to identify the Doe defendant, and there is a risk an ISP will destroy its logs prior to the conference); Melville B. Nimmer & David Nimmer, Nimmer on Copyright, § 14.06[A], at 14-03 (2003). See also attached Nicolini Declaration, paragraph 27.*

Since the identifying records will likely be destroyed before a 26(f) Conference (which can only take place once Plaintiff obtains Defendants' identities from their ISPs), there is good cause to grant the Motion.

4. Plaintiffs' Interest in Knowing Defendants' Identities Outweighs Defendants' Interests in Remaining Anonymous

Plaintiff has a strong interest in protecting its copyrights. All Defendants are alleged copyright infringers who have no legitimate expectation of privacy in the subscriber information they provided to the ISPs, much less in distributing the copyrighted work in question without permission. *See Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 8-9 (D.D.C. Apr. 28, 2008) (Kollar-Kotelly, J.) (finding that the "speech" at issue was that doe defendant's alleged infringement of copyrights and that "courts have routinely held that a defendant's First Amendment privacy interests are exceedingly small where the 'speech' is the alleged infringement of copyrights"); *Interscope Records v. Does 1-14*, 558 F.Supp.2d 1176, 1178 (D.

Kan. 2008) (a person using the Internet to distribute or download copyrighted music without authorization is not entitled to have their identity protected from disclosure under the First Amendment); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) ("computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator"); and *Sony Music Entertainment, Inc. v. Does 1–40*, 326 F.Supp.2d 556, 566 (S.D.N.Y. 2004) ("defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission.")

Since Defendants do not have a legitimate interest in remaining anonymous and Plaintiff has a strong, statutorily recognized interest in protecting its copyrights, Plaintiff has established good cause.

III. CONCLUSION

Based on the above-stated reasons, Plaintiff respectfully requests this Court to grant leave to issue Rule 45 subpoenas to the ISPs set forth on Exhibit A to the Complaint, as well as to any intermediary ISPs that may be identified in the process.

Respectfully submitted this 10th day of January, 2012.

FOR THE PLAINTIFF:

By: /s/ Mike Meier
Mike Meier (NY Bar ID 321277)
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

Attachments:

(1) *Declaration of Jon Nicolini* in Support of Plaintiff's Motion For Leave to Take Discovery Prior to a Rule 26(f) Conference ("Nicolini Declaration") to corroborate the statements in this Memorandum.