IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHER DISTRICT OF ILLINOIS, EASTERN DIVISION

ZAMBEZIA FILM (PTY), Ltd., A South African Corporation	)	
Plaintiff,	)	Case No. 13 cv 1321
v.	)	
JOHN DOES 1-65	)	
Defendants	)	

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

I. Introduction

Plaintiff, a film producer and motion picture copyright holder, filed a Complaint to stop Defendants from copying and distributing to others over the Internet unauthorized copies (files) of the motion picture for which it holds the exclusive licensing and copyrights, specifically "Adventures in Zambezia" (the "Motion Picture"). Using so-called "peer-to-peer" ("P2P") file "swapping" networks, Defendants' infringements allow them and untold others unlawfully to obtain and distribute for free the copyrighted Motion Picture in which Plaintiff made a substantial financial investment to create. Plaintiff sued Defendants as "Doe" Defendants because Defendants committed infringement using on-line pseudonyms ("user names" or "network names"), not their true names. At this point, Plaintiff has only been able to identify the Doe Defendants by (1) their Internet Protocol ("IP") addresses, (2) the dates and times of the alleged infringement, (3) the hash value which identifies each Defendant as participating in the same swarm and (4) the location of each IP address within the State of Illinois.

The only way that Plaintiff can determine Defendants' actual names is from the non-party Internet Service Providers ("ISPs") to which Defendants subscribe and from which Defendants obtain Internet access, as this information is readily available to the ISPs from documents they

keep in the regular course of business. Accordingly, Plaintiff seeks leave of Court to serve limited discovery prior to a Rule 26(f) conference on the non-party ISPs solely to determine the true identities of the Doe Defendants, along with any other infringers who Plaintiff identifies during the course of this litigation, as Plaintiff's infringement monitoring efforts are ongoing and continuing. Plaintiff requests that the Court enter an order allowing Plaintiff to serve Rule 45 subpoenas on the ISPs immediately and requiring the ISPs to comply with the subpoenas.[1]

If the Court grants this Motion, Plaintiff will serve subpoenas on the ISPs requesting the identifying information of the Doe Defendants. If the ISPs cannot themselves identify one or more of the Doe Defendants but can identify an intermediary ISP as the entity providing online services and/or network access to such Defendants, Plaintiff will then serve a subpoena on that ISP requesting the identifying information for the relevant Doe Defendants. In either case, these ISPs will be able to notify their subscribers that this information is being sought, and, if so notified, each Defendant will have the opportunity to raise any objections before this Court. Thus, to the extent that any Defendant wishes to object, he or she will be able to do so.

II. Argument

A. Precedent Allowing Discovery to Identify Doe Defendants

Courts routinely allow discovery to identify "Doe" defendants. See, e.g., Murphy v. Goord, 445 F.Supp.2d 261, 266 (W.D.N.Y. 2006) (in situations where the identity of the alleged defendants may not be known prior to the filing of a complaint, the plaintiff should have an opportunity

---

1 Because Plaintiff does not currently know the identity of any of the Defendants, Plaintiff cannot ascertain the position of any Defendant to this Motion or serve any of the Defendants with a copy of this Motion.

to pursue discovery to identify the unknown defendants); Wakefield v. Thompson, 177 F.3d 1160, 1163 (9th Cir. 1999) (error to dismiss unnamed defendants given the possibility that

identity could be ascertained through discovery); Valentin v. Dinkins, 121 F.3d 72, 75-76 (2d Cir. 1997) (plaintiff should have been permitted to conduct discovery to reveal the identity of defendant); Dean v. Barber, 951 F.2d 1210, 1215 (11th Cir. 1992) (error to deny plaintiff's motion to join John Doe defendant where the identity of John Doe could have been determined through discovery); Munz v. Parr, 758 F.2d 1254, 1257 (8th Cir. 1985) (error to dismiss claim merely because defendant was unnamed; "Rather than dismissing the claim, the court should have ordered disclosure of Officer Doe's identity"); Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir. 1980) ("where the identity of the alleged defendants [are not] known prior to the filing of a complaint . . . the plaintiff should be given an opportunity through discovery to identify the unknown defendants"); Maclin v. Paulson, 627 F.2d 83, 87 (7th Cir. 1980) (where "party is ignorant of defendants' true identity . . . plaintiff should have been permitted to obtain their identity through limited discovery"); Equidyne Corp. v. Does 1-21, 279 F. Supp. 2d 481, 483 (D. Del. 2003) (allowing pre-Rule 26 conference discovery from ISPs to obtain the identities of users anonymously posting messages on message boards).

In similar copyright infringement cases brought by motion picture studios and record companies against Doe defendants, courts have consistently granted plaintiffs' motions for leave to take expedited discovery to serve subpoenas on ISPs to obtain the identities of Doe Defendants prior to a Rule 26 conference. See Warner Bros. Records, Inc. v. Does 1-6, 527 F.Supp.2d 1, 2 (D.D.C. 2007) (allowing plaintiffs to serve a Rule 45 subpoena upon Georgetown University to obtain the true identity of each Doe defendant, including each defendant's true name, current and permanent addresses and telephone numbers, email address, and Media Access Control ("MAC") address) (citing Memorandum Opinion and Order, UMG Recordings,

Inc. v. Does 1-199, No. 04-093(CKK) (D.D.C. March 10, 2004); Order, UMG Recordings v. Does 1-4, 64 Fed. R. Serv. 3d (Callaghan) 305 (N.D. Cal. March 6, 2006)).

In fact, for the past few years, federal district courts throughout the country, including this Court, have granted expedited discovery in Doe Defendant lawsuits that are factually similar to the present lawsuit.[2] In these cited cases and others like them, copyright holder plaintiffs have obtained the identities of P2P network users from ISPs through expedited discovery using information similar to that gathered by Plaintiff in the present case, and they have used that information as the basis for their proposed subpoenas to these ISPs.

Courts consider the following factors when granting motions for expedited discovery to identify anonymous Internet users: (1) whether the plaintiff can identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court; (2) all previous steps taken by the plaintiff to identify the Doe Defendant; and (3) whether the plaintiff's suit could withstand a motion to dismiss.

Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999); see also Rocker Mgmt. LLC v. John Does, No. 03-MC-33 2003 WL 22149380, *1-2, (N.D. Cal. 2003) (applying Seescandy.com standard to identify persons who posted libelous statements on Yahoo!

---

2 Representative cases include First Time Videos, LLC v. Does 1-76, Case No. 11 C 3831 (N.D. Ill.) (Bucklo, J.); Pacific Century Int'l, Ltd. v. Does 1-31, Case No. 11 C 9064 (N.D. Ill.) (Leinenweber, J.); Hard Drive Productions v. Does 1-48, Case No. 11 C 9062 (N.D. Ill.) (Kim, J.); Pacific Century Int'l, Ltd. v. Does 1-25, Case No. 12 C 1535 (N.D. Ill.) (Bucklo, J.); Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 7 (D.D.C. Apr. 28, 2008) (Kollar-Kotelly, J.); Worldwide Film Entertainment LLC v. Does 1-749, Case No. 10-38 (D.D.C.) (Kennedy, Jr., J.); G2 Productions LLC v. Does 1-83, Case No. 10-41 (D.D.C.) (Kollar-Kotelly, J.); Call of the Wild Movie, LLC v. Does 1-358, Case No. 10-455 (D.D.C.) (Urbina, J.); Maverick Entertainment Group, Inc. v. Does 1-1,000, Case No. 10-569 (D.D.C.) (Leon, J.); Donkeyball Movie, LLC v. Does 1-171, Case No. 10-1520 (D.D.C.) (Sullivan, J.).

message board; denying request for expedited discovery where the postings in question were not libelous). Plaintiff here is able to demonstrate each one of these factors.

Overall, courts have wide discretion in discovery matters and have also allowed expedited discovery when "good cause" is shown. See Warner Bros. Records, Inc. v. Does 1-6, 527 F.Supp.2d 1, 2 (D.D.C. 2007); Semitool, Inc. v. Tokyo Electron Am., Inc., 208 F.R.D. 273, 275-76 (N.D. Cal. 2002); Qwest Comm. Int'l, Inc. v. WorldQuest Networks, Inc., 213 F.R.D. 418, 419 (D. Colo. 2003); Entm't Tech. Corp. v. Walt Disney Imagineering, No. Civ. A. 03-3546, 2003 WL 22519440, at *4 (E.D. Pa. Oct. 2, 2003) (applying a reasonableness standard: "a district court should decide a motion for expedited discovery on the entirety of the record to date and the reasonableness of the request in light of all of the surrounding circumstances") (quotations omitted); Yokohama Tire Corp. v. Dealers Tire Supply, Inc., 202 F.R.D. 612, 613-14 (D. Ariz. 2001) (applying a good cause standard).

B. Overview of Plaintiff's Allegations and Factual Showings

As alleged in the complaint, the Doe Defendants, without authorization, used an online media distribution system to download the copyrighted Motion Picture and distribute it to other users on the P2P network, including by making the copyrighted Motion Picture for which Plaintiff holds the exclusive reproduction and distribution rights. See Complaint at para. 14. In the present case, Plaintiff has engaged Crystal Bay Corporation ("CBC"), a provider of online antipiracy services for the motion picture industry, to monitor this infringing activity. See Declaration of Darren M. Griffin ("Griffin Decl."), attached to this Memorandum as Exhibit A.

An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). In logs kept in the ordinary course of business, ISPs maintain records of the IP addresses assigned to their subscribers. Once provided

with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the user/subscriber. (Griffin Decl., para. 4).

Only the ISP that has assigned a particular IP address for use by a subscriber can correlate that IP address to a specific subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses by their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was used. Unfortunately, many ISPs only retain the information necessary to correlate an IP address to a particular subscriber for a very limited period of time. (Id. at para. 5).

Plaintiff retained Crystal Bay Corporation ("CBC"), a company incorporated in South Dakota, to identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted movie as identified in Exhibit A (the "Work"). Darren Griffin, a software consultant with CBC, was responsible for reviewing, analyzing and attesting to the results of the investigation. (Griffin Decl., para. 6).

Forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions (Id. at para. 7) and the transactions and the IP addresses of the users responsible for copying and distributing the Work were isolated. (Id. at para. 8).

Through each of the transactions, the computers using the IP addresses identified in Exhibit B transmitted a copy or a part of a copy of a digital media file identified by the relevant hash value. The IP addresses, hash values, dates and times contained in Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit B were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the copyrighted work. (Griffin Decl., para. 9).

Moreover, the users were sharing the identical copy of the Work. A digital copy of an audiovisual work can be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a US government standard. Using a hash tag to identify different copies of the Work, it was confirmed that these users reproduced the very same copy of the Work. (Id. at para. 10).

The CBC software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture. (Griffin Decl., para. 11).

The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Exhibit B were located in Illinois and, based on information and belief, those users were specifically located in the Northern District of Illinois. Although an IP address alone does not reveal the name or contact information of the subscriber, it does reveal the location of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These Registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. The geographic location of an IP address can be further narrowed by crossreferencing this information with secondary sources such as data contributed to commercial database by ISPs. (Id. at para. 12).

As set forth in Exhibit A, it was confirmed not only that the users distributed the files in Illinois, but also the specific location (city/town) where the distribution took place. (Id. at para. 13).

C. Plaintiff has Shown Good Cause for the Discovery and has made a Prima Facie Showing that Defendants Infringed Plaintiff's Copyright

First, Plaintiff has sufficiently identified the Doe Defendants through the unique IP address that each Doe Defendant was assigned at the time of the unauthorized distribution of the copyrighted Motion Picture. See Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. at 578- 80. These Defendants gained access to the Internet through their respective ISPs (under cover of an IP address) only by setting up an account with the various ISPs. The ISPs can identify each Defendant by name through the IP address by reviewing its subscriber activity logs. Thus, Plaintiff can show that all Defendants are "real persons" whose names are known to the ISP and who can be sued in federal court.

Second, Plaintiff has specifically identified the steps taken to identify Defendants' true identities. Plaintiff has obtained each Defendant's IP address and the date and time of the Defendant's infringing activities, has traced each IP address to specific ISPs, and has made copies of the Motion Picture each Defendant unlawfully distributed or made available for distribution. Therefore, Plaintiff has obtained all the information it possibly can about the Defendants without discovery from the ISPs.

Third, Plaintiff has asserted a prima facie claim for direct copyright infringement in its Complaint that can withstand a motion to dismiss. Specifically, Plaintiff has alleged that: (a) it owns the exclusive rights under the registered copyright for the Motion Picture, and (b) the Doe Defendants copied or distributed the copyrighted Motion Picture without Plaintiff's authorization. See Complaint, at para. 12-16. These allegations state a claim for copyright

infringement. See 17 U.S.C. §106(1)(3); In re Aimster Copyright Litig., 334 F.3d 643, 645 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004) ("Teenagers and young adults who have access to the Internet like to swap computer files containing popular music. If the music is copyrighted, such swapping, which involves making and transmitting a digital copy of the music, infringes copyright."); A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014-15 (9th Cir. 2001) ("Napster users who upload file names to the search index for others to copy violate plaintiffs' distribution rights. Napster users who download files containing copyrighted music violate plaintiffs' reproduction rights").

Here, good cause exists because ISPs typically retain user activity logs containing the information sought for a limited period of time before erasing the data. If that information is erased, Plaintiff will have no ability to identify the Defendants, and thus will be unable to pursue its lawsuit to protect its copyrighted work. Where "physical evidence may be consumed or destroyed with the passage of time, thereby disadvantaging one or more parties to the litigation," good cause for discovery before the Rule 26 conference exists. Qwest Comm., 213 F.R.D. at 419; see also Pod-Ners, LLC v. Northern Feed & Bean of Lucerne LLC, 204 F.R.D. 675, 676 (D. Colo. 2002) (allowing discovery prior to Rule 26 conference to inspect items in defendant's possession because items might no longer be available for inspection if discovery proceeded in the normal course).

Good cause exists here for the additional reason that a claim for copyright infringement presumes irreparable harm to the copyright owner. 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); Elvis Presley Enter., Inc. v. Passport Video, 349 F.3d 622, 631 (9th Cir. 2003). The first and necessary step that Plaintiff must take to stop the infringement of its valuable copyrights and exclusive licensing and distribution rights is to identify the Doe Defendants who are copying and distributing the Motion Picture. This lawsuit cannot proceed without the limited discovery Plaintiff seeks because the ISPs are the only entities that can identify the otherwise anonymous Defendants. Courts regularly permit early discovery where such discovery will "substantially contribute to moving th[e] case forward." Semitool, 208 F.R.D. at 277.

Finally, Defendants have no legitimate expectation of privacy in the subscriber information they provided to the ISPs much less in downloading and distributing the copyrighted Motion Picture without permission. See 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); see also 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"); 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"); Sony Music Entm't, 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"); Arista Records, LLC v. Doe No. 1, 254 F.R.D. 480, 481 (E.D.N.C. 2008); U.S. v. Hambrick, 55 F. Supp. 2d 504, 508

(W.D. Va. 1999), aff'd, 225 F.3d 656 (4th Cir. 2000). This is because a person can have no legitimate expectation of privacy in information he or she voluntarily communicates to third parties. See, e.g., Smith v. Maryland, 442 U.S. 735, 743-44 (1979); U.S. v. Miller, 425 U.S. 435, 442-43 (1976); Couch v. U.S., 409 U.S. 322, 335-36 (1973); Guest v. Leis, 255 F.3d at 335; U.S. v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); U.S. v. Hambrick, 55 F. Supp. 2d at 508.

Although Defendants copied and distributed the Motion Picture without authorization using fictitious user names, their conduct was not anonymous. Using publicly available technology, the unique IP address assigned to each Defendant at the time of infringement can be readily identified. When Defendants entered into a service agreement with the ISPs, they knowingly and voluntarily disclosed personal identification information. As set forth above, this identification information is linked to the Defendant's IP address at the time of infringement, and recorded in the ISP's respective subscriber activity logs. Because Defendants can, as a consequence, have no legitimate expectation of privacy in this information, this Court should grant Plaintiff leave to seek expedited discovery of that information. Absent such leave, Plaintiff will be unable to protect its copyrighted Motion Picture from continued infringement.

Where federal privacy statutes authorize disclosure pursuant to a court order, courts have held that a plaintiff must make no more than a showing of relevance under the traditional standards of Rule 26. See Laxalt v. McClatchy, 809 F.2d 885, 888 (D.C. Cir 1987) (court found "no basis for inferring that the statute replaces the usual discovery standards of the FRCP . . . with a different and higher standard"); Pleasants v. Allbaugh, 208 F.R.D. 7, 12 (D.D.C. 2002); accord Lynn v. Radford, No. 99-71007, 2001 WL 514360, at *3 (E.D. Mich. 2001); Gary v. United States, No. 3:97-CV-658, 1998 WL 834853, at *4 (E.D. Tenn.); see also In re Gren, 633 F.2d 825, 828 n.3 (9th Cir. 1980) ("court order" provision of Fair Credit Reporting Act requires

only "good faith showing that the consumer records sought are relevant") (internal quotation omitted). Plaintiff clearly has met that standard, as the identity of Defendants is essential to Plaintiff's continued prosecution of this action.

III. Conclusion

For the foregoing reasons, Plaintiff respectfully submits that the Court should grant the pending Motion for Leave to Take Discovery Prior to the Rule 26 Conference. Plaintiff requests permission to serve a Rule 45 subpoena on the ISPs it has identified as of this date, and those it identifies in the future, so that the ISPs can divulge the true name, address, telephone number, e-mail address, and MAC address of each Doe Defendant that Plaintiff has identified to date, and those it identifies in the future during the course of this litigation and an order that the ISPs shall comply with the subpoenas. To the extent that any ISP, in turn, identifies a different entity as the ISP providing network access and online services to the Doe Defendants, Plaintiff also seeks leave to serve, on any such later identified ISP, limited discovery sufficient to identify the Doe Defendant prior to the Rule 26 conference.

Plaintiff will only use this information to prosecute its claims. Without this information, Plaintiff cannot pursue its lawsuit to protect its Motion Picture from past and ongoing, repeated infringement.

Date: February 22, 2013

Respectfully submitted,

By: /s/ Matthew Lee Stone /s/
One of the attorneys for Plaintiff

Matthew Lee Stone (ARDC # 6297720)
SCHNEIDER & STONE LLP
8424 Skokie Blvd.
Suite 200
Skokie, Illinois 60077
(847) 933-0300 Telephone
(847) 626-2676 Facsimile
mstone@windycitylawgroup.com