IN THE UNITED STATES DISTRICT
SOUTHERN DISTRICT OF OHIO

LHF PRODUCTIONS, INC. **318 N. Carson St. # 208** **Carson City, Nevada 89701** **Plaintiff,** **Vs.** **JOHN DOES 1-17** **Defendants**.	)	**CASE NO. 2:16-CV-498** **JUDGE Edmund A. Sargus**

PLAINTIFF'S *EX PARTE* APPLICATION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

Plaintiff, by counsel, pursuant to the Federal Rules of Civil Procedure, respectfully moves this Court for leave to take discovery prior to the Rule 26(f) conference for good cause as stated in its accompanying Memorandum in Support filed contemporaneously herewith. A proposed entry will be submitted to chambers for the Court's consideration.

Respectfully Submitted,

Timothy A. Shimko (0006736)
Shimko Law Offices LLC
1010 Ohio Savings Plaza
1801 E. 9th St.
Cleveland, Ohio 44114
Tel. (216) 241-8300
Fax (216) 539-2015
tas@shimkolaw.com

MEMORANDUM IN SUPPORT

I. INTRODUCTION

Plaintiff, a film producer, filed a Complaint seeking damages and injunctive relief related to Defendants' wrongful copying and distribution to others over the Internet of unauthorized copies (files) of a film known as "*Fathers & Daughters"* (the "Motion Picture") for which Plaintiff holds the exclusive copyright. Plaintiff seeks leave to take immediate discovery on third party Internet Service Providers ("ISPs") to determine the true identities of the "Doe" Defendants. Without such discovery, Plaintiff cannot identify the Defendants, and thus cannot pursue its lawsuit or protect its copyright from ongoing infringement. In addition, as more fully explained below, time is of the essence with respect to the information that Plaintiff seeks as it may only be available for a limited time, after which it will be permanently unavailable. If that occurs, the identities of the infringers will never be known. In addition, Plaintiff needs this information immediately because the infringements are ongoing and continuing to damage Plaintiff. Therefore, there is a critical need for limited, immediate discovery as sought in this motion.

Defendants' use of so-called "peer-to-peer" ("P2P") "file swapping" networks, allow Defendants and untold others to unlawfully obtain and distribute Plaintiff's Motion Picture for free. Plaintiff named Defendants as "Doe" because Defendants committed their infringements using on-line pseudonyms ("user names" or "network names"), not their true names. To date, Plaintiff has only been able to identify the Doe Defendants by their Internet Protocol ("IP") address and the date and time of the infringement.

The only way that Plaintiff can determine Defendants' actual names is from the non-party 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, contact information, and other identifying information of the Doe Defendants, as well as any other infringers that Plaintiff identifies during the course of this litigation, as Plaintiff's infringement monitoring efforts are on-going and continuing. Accordingly, Plaintiff requests that the Court enter an order allowing Plaintiff to serve Rule 45 subpoenas on the ISPs immediately and that the ISPs shall comply with the subpoenas.1

If the Court grants this Motion, Plaintiff will serve subpoenas on the ISPs requesting the identifying information. 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 any 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.2

II. ARGUMENT

A. PRECEDENT ALLOWS 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 alleged

1 Because Plaintiff does not currently know the identity of any of the Defendants, Plaintiff cannot serve any of the Defendants with this Motion.

2 As further explained below, to the extent that any one or more of the ISP's or unknown intermediary ISPs are educational institutions, this motion is further being made pursuant to 20 USC § 1232g(b)(2)(B).

defendants may not be known prior to the filing of a complaint, the plaintiff should have an opportunity 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 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 identity of defendant); Dean v. Barber, 951 F.2d 1210, 1215-16 (11th Cir. 1992) (error to deny plaintiff's motion to join John Doe defendant where 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 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 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 BMG Music, et al. v. Does 1-9; filed in this Court, Case No. 2:07-CV-00961-JLG-MRA (S.D. Ohio Oct. 16, 2007) (Docs 4-6), and other cases filed in this district and else ware including: Arista Record LLC v. Does 1-4, Case No. 2:05-cv-0227 (S.D.

Ohio June 9, 2005); Capitol Records, Inc. V. Doe, Case No. 4:04-cv-90 (E.D. Tenn. Nov. 15, 2004); Warner Bros. Records Inc. v. Does 1-35, No. 2:04-cv-00084-WOB (E.D. Ky. May 4, 2004); Warner Bros. Records Inc. v. Does 1-9, No. 04-71058 (E.D. Mich. April 5, 2004); BMG Music v. Does 1-9, No 5:04-cv-58 (W.D. Mich. May 6, 2004; Interscope Records v. Does 1-7, No. 2-04-0240 (M.D. Tenn. Mar. 29, 2004; Warner Bros. Records Inc. v. Does 1-6, 527 F. Supp. 2d 1, 2-3 (D.D.C. 2007) (citing Memorandum Opinion and Order, UMG Recordings, Inc. v. Does 1-199, No. 04-093 (CKK) (D.D.C. Mar. 10, 2004); Order, UMG Recordings v. Does 1-4, 64 Fed. R. Serv. 3d (West) 305 (N.D. Cal. 2006)) (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).

In fact, federal district courts throughout the country, including this Court, have routinely granted expedited discovery in Doe Defendant lawsuits that are factually similar to the instant lawsuit.3 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 instant case, and they have used that information as the basis for their proposed subpoenas to these ISPs.

3 Such cases include Cornered, Inc. v. Does 1-2177, Civil Action No. 10-01476 (CKK) (D.D.C. Oct. 22, 2010); Donkeyball Movie, LLC v. Does 1-171, Civ. Action No. 10-1520 (EGS) (D.D.C. Oct. 19, 2010); Voltage Pictures, LLC v. Does 1-5,000, Civil Action No. 10-00873 (D.D.C. June 25, 2010); Maverick Entm’t Group, Inc. v. Does 1-1,000, Civil Action No. 10-569 (D.D.C. Apr. 19, 2010); Call of the Wild Movie, LLC v. Does 1-358, Civil Action No. 10-455 (RMU) (D.D.C. Apr. 15, 2010); West Bay One, Inc. v. Does 1- 2,000, Civil Action No. 10-0481 (JDB) (D.D.C. Apr. 13, 2010); Worldwide Film Entm’t, LLC v. Does 1-749, CA. 1:10-cv-00038-HHK (D.D.C. Jan. 26, 2010); G2 Productions, LLC v. Does 1-83, Civil Action No. 10-041 (D.D.C. Jan. 21, 2010); Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 7 (D.D.C. 2008); Lions Gate Films, Inc. v. Does 1-5, Civ. Action No. 05-386 (EGS) (D.D.C. Mar. 1, 2005); Twentieth Century Fox Film Corp. v. Does 1-9, Civ. Action No. 04-2006 (EGS) (D.D.C. Dec. 15, 2004); Metro-Goldwyn-Mayer Pictures Inc. v. Does 1-10, Civil Action No. 04-2005 (JR) (D.D.C. Nov. 23, 2004); UMG Recordings v. Does 1-199, Civil Action No. 04-093 (CKK) (D.D.C. Mar. 10, 2004).

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. Does 1 Through 20, No. 03-MC-33, 2003 WL 22149380, *1-3, (N.D. Cal. May 29, 2003) (applying Seescandy.com standard to identify persons who posted libelous statements on Yahoo! 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., 527 F. Supp. 2d at 2; Semitool, Inc. v. Tokyo Electron Am., Inc., 208 F.R.D. 273, 275-76 (N.D. Cal. 2002); Qwest Commc'ns 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 and copy 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 sale and distribution rights available for distribution to others. See Complaint at ¶11-14. In the instant case, Plaintiff has engaged Crystal Bay Cooperation ("Crystal Bay"), a provider of online anti-piracy services for the motion picture industry, to monitor this infringing activity. See Declaration of Daniel Macek ("Macek Decl."), ¶2, (attached to this Motion as Exhibit A).

1. Overview of the P2P Infringing Activity

The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. Macek Decl., ¶3. It allows users to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data. Id. The Internet also affords opportunities for the wide-scale infringement of copyrighted motion pictures and other digital content. Macek Decl., at ¶4. Once a motion picture has been transformed into a digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality. Macek Decl., ¶5.

To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called P2P networks. Macek Decl. at ¶6. P2P networks, at least in their most common form, are computer systems that enable Internet users to: (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer

exact copies of files from one computer to another via the Internet. Id. (To use a P2P or BitTorrent distribution system requires more than a click of a button. A software installation and configuration process needs to take place. Macek Decl., par 7). The P2P systems enable widespread distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to other users and so on, so that complete digital copies can be easily and quickly distributed thereby eliminating long download times. Macek Decl. at ¶8.

While Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement. Macek Decl., ¶9. Additionally, the P2P methodologies for which Crystal Bay monitored for Plaintiff's Motion Picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. Macek Decl., ¶10. The initial file-provider intentionally elects to share a file using a P2P network. Id. This is called "seeding." Id. Other users ("peers") on the network connect to the seeder to download. Id. As additional peers request the same file; each additional user becomes a part of the network (or "swarm") from where the file can be downloaded. Id. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole. Id. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a P2P network can also be a source of download for that infringing file, potentially both copying and distributing the infringing Motion Picture. Macek Decl., ¶11.

The distributed nature of P2P leads to a rapid spreading of a file throughout peer users. Id. As more peers join the swarm, the likelihood of a successful download increases. Id. Because

of the nature of a P2P protocol, any seed peer who has downloaded a file is automatically a possible seed source for the subsequent copying. Id.

2. Preliminary Identification of Defendants

All infringers connected to those files are investigated through downloading a part of the file on their computer. Macek Decl., ¶12. This evidence is then saved by Crystal Bay. Macek Decl., ¶13. The forensic software routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works. Macek Decl., ¶15.

An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). Macek Decl., ¶16. It only enables Plaintiff to trace the infringer's access to the Internet to a particular ISP. Id. An ISP can be a telecommunications service provider such as Verizon, an Internet Service Provider such as America Online, a cable Internet Service Provider such as Comcast, or even an entity that is large enough to establish its own network and link directly to the Internet. Id.

In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Macek Decl., ¶17. 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 other related information of the user/subscriber. Id.

Each time a subscriber logs on, he or she may be assigned a different (or "dynamic") IP address unless the user obtains from his/her ISP a static IP address. Macek Decl., ¶16. ISPs are assigned certain blocks or ranges of IP addresses by the Internet Assigned Numbers Authority ("IVANA") or a regional internet registry such as the American Registry for Internet Numbers

("ARIN"). Id.

Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. Macek Decl., ¶18. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Id. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Crystal Bay determined that the Doe Defendants identified in Complaint Exhibit B were using the ISPs listed in the exhibit to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture. Macek Decl., ¶19.

It is possible for digital files to be mislabeled or corrupted, Crystal Bay (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves. Macek Decl., ¶20. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay watches a DVD of the original Motion Picture. Macek Decl., ¶21. After Crystal Bay identified the Doe Defendants and downloaded the motion pictures they were distributing, Crystal Bay opened the downloaded files, watched them and confirmed that they contained the Motion Picture. Macek Decl., ¶22.

After reviewing the evidence logs, isolated the transactions and the IP addresses of the users responsible for copying and distributing the Motion Picture. Macek Decl., ¶24. Through each of the transactions, the computers using the IP addresses identified in Complaint Exhibit B transmitted a copy or a part of a copy of a digital media file of the copyrighted Motion Picture identified by the hash value set forth in Complaint Exhibit B. Macek Decl., ¶25. The IP

addresses, hash values, dates and times contained in Complaint Exhibit B correctly reflect what is contained in the evidence logs. Id. The subscribers using the IP addresses set forth in Complaint Exhibit B were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the copyrighted Motion Picture. Id.

Moreover, the users were sharing the exact same copy of the Motion Picture. Macek Decl., ¶26. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." Id. The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1." Id. By using a hash tag to identify different copies of the Motion Picture, Crystal Bay was able to confirm that these users reproduced the very same copy of the Motion Picture. Id.

The Crystal Bay software analyzed each BitTorrent "piece" distributed by each IP address listed in Complaint Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture file. Macek Decl., ¶27. The software uses a geolocation functionality to determine the location of the IP addresses under investigations. Macek Decl., ¶28. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. Id. These registries assign blocks of IP addresses to ISPs by geographic region. Id. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly- available and searchable format. Id. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs. Id.

Specifically, Plaintiff requests leave to serve subpoenas on the ISPs listed in Exhibit 1

and any intermediary ISPs or other ISPs later identified with respect to any ongoing infringements.

C. PLAINTIFF HAS SHOWN GOOD CAUSE FOR EXPEDITED DISCOVERY AND HAS MADE A PRIMA FACIE SHOWING THAT DEFENDANTS DID INFRINGE PLAINTIFF'S COPYRIGHTS.

First, Plaintiff has sufficiently identified the Doe Defendants through the unique IP address each Doe Defendant was assigned at the time of the unauthorized distribution of the copyrighted Motion Picture. See Columbia Ins. Co., 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 each Defendant's infringing activities, traced each IP address to specific ISPs, and made copies of the Motion Picture each Defendant unlawfully distributed or made available for distribution. Therefore, Plaintiff has diligently 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 and established that: (a) it owns the exclusive rights under the registered copyright attached as Exhibit A for the Motion Picture, and (b) the Doe Defendants copied or distributed the copyrighted Motion Picture without Plaintiff's authorization. See Complaint, ¶¶ 11-17. These

allegations state a prima *facie claim* for copyright infringement. See 17 U.S.C. §106(1)(3); In re Amstar 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 (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."); 17 U.S.C §410.

Here, good cause exists because ISPs typically retain user activity logs containing the information sought for only 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. "[W]here 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 may exist. Qwest Commc'ns, 213 F.R.D. at 419; see also Pod-Ners, LLC v. Northern Feed & Bean of Lucerne Ltd. Liability Co., 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, No. C 08-1193 SBA, 2008 WL 4104214, at *5 (N.D. Cal. Sept. 3, 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 Enters., 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.

Moreover, good cause exists here because there is a very real danger that the ISP will not long preserve the information that plaintiffs seek. ISP's typically retain user activity logs containing the information sought for only a limited period of time before erasing the data. Once the information is gone, Plaintiff will never be able to identify the infringing Defendants.

In addition, good cause exists because the narrowly-tailored discovery requests do not exceed the minimum information required to advance this lawsuit and will not prejudice the Defendants. Semitool, 208 F.R.D. at 276. There is no prejudice to defendants because Plaintiff only seeks the information necessary to identify and serve them, and Plaintiff agrees to use the information disclosed pursuant to the subpoenas only for the purposes of protecting their rights under copyright laws.

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, 1178-79 (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 at 8-9 (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); United States 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); United States v. Miller, 425 U.S. 435, 442-43 (1976); Couch v. United States, 409 U.S. 322, 335-36 (1973); Guest, 255 F.3d at 335; United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); Hambrick, 55 F. Supp. 2d at 508.

Although the 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 to it. 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, as a consequence, have no legitimate expectation of privacy in this information, this Court should grant Plaintiff leave to seek expedited discovery of it. Absent such leave, Plaintiff will be unable to protect its copyrighted Motion Picture from continued infringement.

Plaintiff also requests that that the Court make clear that with respect to any ISPs that are federally-funded educational institutions pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g ("FERPA"), that their obligations to respond to subpoena are consistent with their obligations pursuant to FERPA. Though the FERPA generally prohibits disclosure of certain records by federally-funded educational institutions, it expressly provides that information can be disclosed pursuant to court order. See 20 U.S.C. 1232g(b)(2)(B). While Plaintiff does not believe FERPA prevents the

disclosure of the information requested, universities and colleges have expressed concern about their obligations under FERPA, and some have taken the position that a court order is required before they will disclose subscriber information. Hence, Plaintiff seeks an appropriate order explicitly authorizing all ISP's otherwise subject to FERPA to comply with the subpoena.

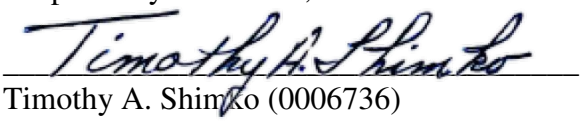
III. CONCLUSION

For the foregoing reasons, Plaintiff respectfully submits that good cause exists, and therefore this Court should grant Plaintiff's *Ex Parte* Application for Leave to Take Discovery Prior to Rule 26(F) Conference and enter an Order substantially in the form of the Proposed Order being submitted in connection with this Motion. 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(es), telephone number(s), e-mail address(es),

and Media Access Control Number ("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. Finally, Plaintiff requests that the order specify that to the extent applicable, that the ISPs disclose the information pursuant to FERPA (20 U.S.C. 1232g).

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.

Respectfully Submitted,



Timothy A. Shimko (0006736)
Shimko Law Offices LLC
1010 Ohio Savings Plaza
1801 E. 9th St.
Cleveland, Ohio 44114
Tel. (216) 241-8300
Fax (216) 539-2015
tas@shimkolaw.com

Attorneys for Plaintiff

EXHIBIT A

Declaration of *Daniel Macek*

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

Dallas Buyers Club, LLC
2170 Buckthorne Place, Suite 400 The Woodlands, TX 77380

Plaintiff,

V.

DOES 1- 35,

Defendants.

Case No.: 2:14-cv-388

Judge: Edmund Sargus

Magistrate Judge: Norah McCann King

DECLARATION OF DANIEL MACEK PURSUANT TO 28 U.S.C. § 1746
IN SUPPORT OF PLAINTIFF'S *EX PARTE* APPLICATION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

1. My name is Daniel Macek. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

2. I have been retained as a consultant by Crystal Bay Corporation ("Crystal Bay"), a company incorporated in South Dakota and organized and existing under the laws of the United States, in its technical department. Crystal Bay is in the business of providing forensic investigation services to copyright owners.

3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows users to freely and easily exchange ideas and information, including academic research, literary works, financial

data, music, audiovisual works, graphics, and an unending and ever-changing array of other data.

4. The Internet also affords opportunities for the wide-scale infringement of copyrighted motion pictures and other digital content.

5. Once a motion picture has been transformed into a digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called peer-to peer ("P2P") or BitTorrent networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. To use a P2P or BitTorrent distribution system requires more than a click of a button. A substantial software installation and computer configuration process needs to take place.

8. The P2P systems enable widespread distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to other users and so on, so that complete digital copies can be easily and quickly distributed thereby eliminating long download times.

9. While Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies for which Crystal Bay monitored for Plaintiff's Motion Picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file using a P2P network. This is called "seeding." Other users ("peers") on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or "swarm") from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together to comprise the whole.

11. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a P2P network can also be a source of download for that infringing file, potentially both copying and distributing the infringing Motion Picture. The distributed nature of P2P leads to rapid spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent.

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence is then saved on a secure server.

14. Once the searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, it automatically obtains the IP address of a user offering the file

for download and saves it in a secure database.

15. The forensic software routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works. In this way the software is connected to files of illegal versions of the Motion Picture.

16. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). It only enables Plaintiff to trace the infringer's access to the Internet to a particular ISP. An ISP can be a telecommunications service provider such as Verizon, an Internet Service Provider such as America Online, a cable Internet Service Provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet. Each time a subscriber logs on, he or she may be assigned a different (or "dynamic") IP address unless the user obtains from his or her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses by the Internet Assigned Numbers Authority ("IANA") or a regional internet registry such as the American Registry for Internet Numbers ("ARIN"). However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. These intermediaries can be identified by the ISP and the intermediaries' own logs will contain the subscriber information.

17. In logs kept in the ordinary course of business, ISPs keep track 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 other related information of the user/subscriber.

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used.

19. Crystal Bay Cooperation determined that the Doe Defendants identified in Complaint Exhibit B were using the ISPs listed in the exhibit to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

20. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves.

21. As to Plaintiffs copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay watches a DVD of the original Motion Picture.

22. After Crystal Bay identified the Doe Defendants' IP Addresses and downloaded the motion pictures they were distributing, Crystal Bay opened the downloaded files, watched them and confirmed that they, in fact, contained the Motion Picture identified in the Complaint.

23. To identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiffs copyrighted Motion, Crystal Bay Corporation's forensic software scans peer-to-peer networks for the presence of infringing transactions.

24. After reviewing the evidence logs, I isolated the transactions and the IP

addresses of the users responsible for copying and distributing the Motion Picture.

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

26. Moreover, the users were sharing the exact same copy of the Motion Picture. Any digital copy of an audiovisual work may 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". By using a hash tag to identify different copies of the Motion Picture, Crystal Bay is able to confirm that these users reproduced the very same copy of the Motion Picture.

27. The Crystal Bay software analyzed each BitTorrent "piece" distributed by each IP address listed in Complaint Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

28. The software uses a geolocation functionality to determine the location of the IP addresses under investigations. The location of each IP address is set forth in Complaint Exhibit 1. 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. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and

searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION:

PURSUANT TO 28 U.S.C. § 1746, I, Daniel Macek, hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 30 day of April, 2014.

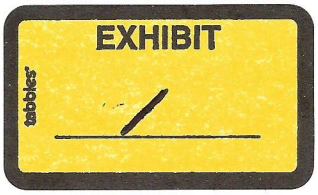
By: _____
Daniel Macek

SHA1: 3DAAD5C4A9E96E8229E553877CC4B79CE1E4E6A3

FILM TITLE: LONDON HAS FALLEN

RIGHTS OWNER: LONDON HAS FALLEN PRODUCTIONS, INC.

John Doe #	IP	Port	Client	Hit Date UTC	ISP	City
1	75.118.31.114	49872	[unknown Client]	2016-04-23 12:37:03	WideOpenWest	Columbus
2	74.83.43.178	50682	µTorrent 2.2.1	2016-04-22 13:39:19	Fuse Internet Access	Cincinnati
3	74.215.87.14	43543	[unknown Client]	2016-04-20 23:15:58	Fuse Internet Access	Mason
4	104.169.136.35	19563	BitTorrent 7.9.6	2016-04-20 19:42:49	Frontier Communications	Leesburg
5	75.118.24.239	50322	[unknown Client]	2016-04-19 03:30:37	WideOpenWest	Columbus
6	65.60.244.103	40795	[unknown Client]	2016-04-18 11:24:29	WideOpenWest	Columbus
7	74.199.116.153	55784	[unknown Client]	2016-04-18 05:39:20	WideOpenWest	Columbus
8	104.169.79.211	60383	µTorrent 2.2.1	2016-04-17 02:00:58	Frontier Communications	Circleville
9	208.102.159.5	50321	[unknown Client]	2016-04-16 19:32:01	Fuse Internet Access	Hamilton
10	74.83.111.153	42044	[unknown Client]	2016-04-16 10:32:21	Fuse Internet Access	Bethel
11	74.83.10.82	59449	BitTorrent 7.9.6	2016-04-16 01:25:55	Fuse Internet Access	Cincinnati
12	69.47.139.124	62900	µTorrent 2.2.1	2016-04-15 17:58:29	WideOpenWest	Reynoldsburg
13	104.235.17.202	38418	µTorrent 0.G.0	2016-04-15 06:52:41	Frontier Communications	West Milton
14	104.169.92.53	63737	BitTorrent 7.9.6	2016-04-15 04:34:34	Frontier Communications	Sardinia
15	104.240.172.52	63737	BitTorrent 7.9.6	2016-04-14 21:23:13	Frontier Communications	Caldwell
16	74.215.248.117	31434	µTorrent 3.4.6	2016-04-14 12:10:02	Fuse Internet Access	Cincinnati
17	216.68.52.130	56148	[unknown Client]	2016-04-13 16:53:24	Fuse Internet Access	Cincinnati



THE UNITED STATES DISTRICT COURT
THE SOUTHERN DISTRICT OF OHIO

LHF PRODUCTIONS, INC	)	
	)	
	)	**Case No. 2:16-CV-498**
	)	
Plaintiff,	)	
	)	**Judge Edmund Sargus**
vs.	)	
	)	
	)	
	)	
JOHN DOES 1-17,	)	
	)	
Defendants.	)	

ORDER

This is a copyright action in which plaintiff alleges that defendants "conspired with other infringers on the BitTorrent network to copy and/or distribute" plaintiff's copyrighted motion picture, *London Has Fallen*, Doc. No. 1, ¶¶ 11, 13. Defendants are otherwise identified only by IP addresses. *Exhibit 1*, attached to *Complaint*. This matter is now before the Court on *Plaintiff's Ex Parte Application for Leave to Take Discovery Prior to Rule 26(f) Conference*, Doc. No. 3 ("*Plaintiff's Motion*"). In its motion, plaintiff seeks to conduct limited discovery of non-party internet service providers to determine the identities of the defendants.

The Federal Rules of Civil Procedure prohibit "discovery from any source before the parties have conferred as required by Rule 26(f), except," *inter alia*, when authorized by court order. Fed. R. Civ. P. 26(d)(1). Expedited discovery is appropriate upon a showing of good cause. *Arista Records, LLC v. Does 1-15*, No. 2:07-CV-450, 2007 WL 5254326, at *2 (S.D. Ohio May 17, 2007). Good cause is easily established in a copyright infringement case, *see id.,* where, as here, plaintiff has established that it cannot meet its service obligation under Fed. R.

Civ. P. 4 without the requested discovery.

Accordingly, *Plaintiff's Motion*, Doc. No. 2, is **GRANTED**.

IT IS HEREBY ORDERED that plaintiff may serve limited, immediate discovery on the internet service providers identified in Exhibit 1 attached to *Plaintiff's Motion*, and on later-discovered or intermediary internet service providers in order to obtain the identity of each Doe defendant by serving a Rule 45 subpoena that seeks documents that identify each Doe defendant, including the name, current (and permanent) addresses and telephone numbers, e-mail addresses and Media Access Control addresses for each defendant. The disclosure of this information is ordered pursuant to 20 U.S.C. § 1232g(b)(2)(B) where applicable to educational institutions.

IT IS FURTHER ORDERED THAT any information disclosed to plaintiff in response to the Rule 45 subpoenas may be used by plaintiff solely for the purpose of protecting plaintiff's rights under the Copyright Act.

Date _____

_____
JUDGE