IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 16-cv-01836

CRIMINAL PRODUCTIONS, INC.,
a Nevada corporation

Plaintiff,

vs.

JOHN DOE 1, et.al.,

Defendants.

MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

Plaintiff, by counsel, pursuant to the Federal Rules of Civil Procedure, respectfully move this Court for leave to take discovery prior to the Rule 26(f) conference for the reasons stated in its accompanying Memorandum of Points & Authorities filed contemporaneously herewith. Plaintiff requests a hearing on this matter, if necessary, on an expedited basis.

Respectfully submitted,

Criminal Productions, Inc.,

/s/ Scott T. Kannady
Scott T. Kannady, No. 29995
BROWN & KANNADY, LLC
Attorneys for the Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

CRIMINAL PRODUCTIONS, INC.,
a Nevada corporation

Plaintiff,

vs.

JOHN DOE 1, et.al.,

Defendants.

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Miscellaneous

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiff, 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 "Criminal" (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 that Plaintiff invested substantial sums of money to make. Plaintiff sued Defendants as "Doe" Defendants because Defendants committed their infringements 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 their Internet Protocol ("IP") address and the date and time of alleged infringement.

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 several of the non-party ISPs solely to determine the true identities of the Doe Defendants, as well as any other infringers that Plaintiff identify during the course of this litigation, as Plaintiff's infringement monitoring efforts are on-going and continuing. Therein, 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]

[1] Because Plaintiff does not currently know the identity of any of the Defendants, Plaintiff cannot ascertain any of the Defendants' position on this Motion or serve any of the Defendants with this Motion.

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 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. PRECEDENTS OF COURTS 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 alleged 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 (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 plaintiff's 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 plaintiff 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 have granted expedited discovery in Doe defendant lawsuits that are factually similar to the instant lawsuit.[2]

[2] Such cases include Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 7 (D.D.C. Apr. 28, 2008) (Kollar-Kotelly, J.); Metro-Goldwyn-Mayer Pictures Inc., et al. v. Does 1-10, Case No. 04-2005 (D.D.C.) (Robertson, J.); Twentieth Century Fox Film Corporation, et al. v. Does 1-9, Case No. 04-2006 (D.D.C.) (Sullivan, J.); Lions Gate Films, Inc., et al. v. Does 1-5, Case No. 05- 386 (D.D.C.) (Sullivan, J.); UMG Recordings, et al. v. Does 1-199, Case No. 04-093 (D.D.C.) (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.) (KollarKotelly, J.); Achte/Neunte Boll Kino Beteiligungs GMBH & CO KG v. Does 1- 4,577, Case No. 10-453 (D.D.C.) (Collyer, J.); West Bay One, Inc. v. Does 1- 2,000, Case No. 10-481 (D.D.C.) (Bates, 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.)

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.

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! 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")

(Leon, J.); Voltage Pictures, LLC v. Does 1-5,000, Case No. 10-00873 (D.D.C.) (Urbina, J.); Cornered, Inc. v. Does 1-2,177, Case No. 10-1476 (D.D.C.) (Kollar-Kotelly, J.); Donkeyball Movie, LLC v. Does 1-171, Case No. 10-1520 (D.D.C.) (Sullivan, J.).

(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 sale and distribution rights available for distribution to others. In the instant case, Plaintiff has engaged Maverickeye UG ("MEU"), a provider of online anti-piracy services for the motion picture industry, to monitor this infringing activity. See Declaration of Daniel Macek ("Macek Decl."), ¶¶ 1-2 [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 hundreds of millions of people around the world 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. Unfortunately, the Internet also has afforded opportunities for the wide-scale infringement of copyrighted motion pictures. Macek Decl., ¶ 4. Once a motion picture has been transformed into an unsecured 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., ¶ 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.

At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material. Macek Decl., ¶ 6. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed. Macek Decl., ¶ 8.

Further, a person who uses a P2P network is free to use any alias (or "network name") whatsoever, without revealing his or her true identity to other users. Macek Decl., ¶ 9. Thus, 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. Id.

Additionally, the P2P methodologies for which Maverickeye UG 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—or even a portion of a copy—can also be a source of download for that infringing file, potentially both copying and distributing the infringing work. Macek Decl., ¶ 11.

This distributed nature of P2P leads to a rapid viral 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 prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file. Id.

2. Preliminary Identification of Defendants

On behalf of Plaintiff, Maverickeye UG engaged in a specific process utilizing its specially designed software technology to identify direct infringers of Plaintiff's copyrights using protocols investigated by Maverickeye UG's software on P2P networks. Macek Decl., ¶ 12-14. All of the infringers named as Doe Defendants were identified in the following way: Maverickeye UG software is connected to files of illegal versions of the Motion Picture. Macek Decl., ¶ 15. All infringers connected to those files are investigated through downloading a part of the file placed on their computer. Macek Decl., ¶ 12. This evidence is then saved on Maverickeye UG secure servers. Macek Decl. ¶ 13.

Once Maverickeye UG's searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff own the exclusive licensing and distribution rights, Maverickeye UG obtains the IP address of a user offering the file for download. Macek Decl., ¶ 15. When available, Maverickeye UG also obtains the user's

pseudonym or network name and examines the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's Motion Picture. Macek Decl.; ¶ 19-25. In addition to the file of the motion picture itself, Maverickeye UG downloads or otherwise collects publicly available information about the network user that is designed to help Plaintiff identify the infringer. Id. Among other things, Maverickeye UG downloads or records for each file downloaded: (a) the time and date at which the file or a part of the file was distributed by the user; (b) the IP address assigned to each user at the time of infringement; and, in some cases, (c) the video file's metadata (digital data about the file), such as title and file size, that is not part of the actual video content, but that is attached to or contained within the digital file and helps identify the content of the file. Id. Maverickeye UG then creates evidence logs for each user that store all this information on a secure server. Macek Decl.; ¶13.

An IP address is, in combination with the date, a unique numerical identifier that is automatically assigned to a user by its ISP each time a user logs on to or accesses the network. Macek Decl., ¶ 16. 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. Id. 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"). Id. ISPs keep track of the IP addresses assigned to their subscribers at any given moment and retain such "user logs" and can use these logs to identify the user/ subscriber. Macek Decl., ¶ 17-18. These user logs provide the most accurate means to correlate an infringer's IP address to his or her true identity. Macek Decl., ¶ 18.

Although users' IP addresses are not automatically displayed on the P2P networks, any user's IP address is readily identifiable from the packets of publicly available data being

exchanged. Macek Decl., ¶ 19. The exact manner in which Maverickeye UG determines a user's IP address varies by P2P network. Macek Decl., ¶ 20.

An infringer's IP address is significant because it is becomes a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer using the Internet. Macek Decl., ¶ 16. However, the IP address does not enable Maverickeye UG to ascertain with certainty the exact physical location of the computer or to determine the infringer's identity. Id. It only enables Maverickeye UG to trace the infringer's access to the Internet to a particular ISP. Id. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. 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 such as a university that is large enough to establish its own network and link directly to the Internet. Id.

Here, the IP addresses Maverickeye UG identified for Plaintiff enable Maverickeye UG to determine which ISP was used by each infringer to gain access to the Internet. Macek Decl., ¶ 16. Publicly available databases located on the Internet list the IP address ranges assigned to various ISPs. Id. However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. Id. Since these ISPs consequently have no direct relationship— customer, contractual, or otherwise—with the end-user, they are unable to identify the Doe Defendants through reference to their user logs, but they can identify the intermediary ISP to which that IP address has been allocated. Id. The intermediary ISPs' own user logs, therefore, should permit identification of the Doe Defendants. Id.

Maverickeye UG determined that the Doe Defendants here were using ISPs listed in Exhibit B to Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference,

together with various other ISPs operating both within and outside the Colorado, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture. Macek Decl., ¶ 26. Plaintiff specifically request leave to conduct discovery on all of the Doe Defendants it has been able to identify to date, 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.

Maverickeye UG then downloaded the motion picture file, or a substantial part of it, and other identifying information described above and created evidence logs for each Doe Defendant. Macek Decl., ¶ 20. Once provided with the IP address, plus the date and time of the infringing activity, the Doe Defendant's ISPs quickly and easily can use their respective subscriber logs to identify the name and address of the ISP subscriber who was assigned that IP address at that date and time. Macek Decl., ¶ 17.

Lastly, Maverickeye UG confirms that the digital audiovisual files it downloaded are actual copies of Plaintiff's Motion Picture. Macek Decl., ¶ 20. It is possible for digital files to be mislabeled or corrupted; therefore, Maverickeye UG (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. Id.

As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Maverickeye UG watches a DVD copy of the Motion Picture provided by Plaintiff. Macek Decl., ¶ 21. After Maverickeye UG identified the Doe Defendants and downloaded the motion pictures they were distributing, Maverickeye UG opened the downloaded files, watched them and

confirmed that they contain a substantial portion of the motion picture identified in the Complaint. Macek Decl. ¶ 22.

C. PLAINTIFF HAS SHOWN GOOD CAUSE FOR THE 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. 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, have traced each IP address to specific ISPs, and have 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 have 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. 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 Plaintiff's distribution rights. Napster users who download files containing copyrighted music violate Plaintiff's reproduction rights").

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. 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 thus 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 each 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 it. 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 submit that the Court should grant the Motion for Leave to Take Discovery Prior to Rule 26 Conference. Plaintiff request 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 have 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.

Respectfully submitted this 19 day of July, 2016.

BROWN & KANNADY, LLC

/s/ Scott T. Kannady
Scott T. Kannady, No. 29995
BROWN & KANNADY, LLC
2000 South Colorado Blvd., Suite 2-440
Denver, CO 80222
Phone: (303) 757-3800
Fax: (303) 757-3815
E-mail: scott@brownlegal.com

ATTORNEY FOR PLAINTIFF

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

CRIMINAL PRODUCTIONS, INC.,
a Nevada Corporation,

Plaintiff,

vs.

John Doe 1, et.al.,

Defendants.

DECLARATION OF DANIEL MACEK IN SUPPORT OF PLAINTIFF'S MOTION 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 Maverickeye UG ("MEU"), a company incorporated in Stuttgart and organized and existing under the laws of Germany, in its technical department. MEU 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 software installation and 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 digitial 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 Maverickeye UG 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/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. Maverickeye UG determined that the Doe Defendants identified in Complaint Exhibit A 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, Maverickeye UG (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 Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Maverickeye UG watches a DVD of the original Motion Picture.

22. After Maverickeye UG identified the Doe Defendants and downloaded the motion pictures they were distributing, Maverickeye UG opened the downloaded files, watched them and confirmed that they contained the Motion Picture identified in the Complaint.

23. To identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted Motion Picture, Maverickeye UG'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 A 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 A. The IP addresses, hash values, dates and times contained in Complaint Exhibit A correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Complaint Exhibit A 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, MEU was able to confirm that these users reproduced the very same copy of the Motion Picture.

27. The MEU software analyzed each BitTorrent "piece" distributed by each IP address listed in Complaint Exhibit A 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 A. 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 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 14 day of June, 2016.

By: _____
Daniel Macek

No	IP	Port	Client	Hit Date UTC	File Name
1	50.152.24.2	60310	libtorrent 1.0.0	06/04/2016 20:29:46	Criminal.2016.TS.XviD-VAiN
2	75.173.239.167	40361	µTorrent 3.4.7	06/08/2016 15:58:32	Criminal.2016.TS.XviD-VAiN
3	174.24.101.122	40361	µTorrent 3.4.7	06/09/2016 04:21:54	Criminal.2016.TS.XviD-VAiN
4	75.173.235.94	40361	µTorrent 3.4.7	06/10/2016 12:28:52	Criminal.2016.TS.XviD-VAiN
5	97.121.130.111	40361	µTorrent 3.4.7	06/10/2016 23:26:24	Criminal.2016.TS.XviD-VAiN
6	174.22.179.95	40361	µTorrent 3.4.7	06/11/2016 03:08:46	Criminal.2016.TS.XviD-VAiN
7	97.121.142.96	40361	µTorrent 3.4.7	06/11/2016 19:42:57	Criminal.2016.TS.XviD-VAiN
8	97.121.153.134	40361	µTorrent 3.4.7	06/11/2016 19:48:26	Criminal.2016.TS.XviD-VAiN
9	97.121.184.178	40361	µTorrent 3.4.7	06/18/2016 11:12:18	Criminal.2016.TS.XviD-VAiN
10	71.219.227.130	40361	µTorrent 3.4.7	06/18/2016 17:05:38	Criminal.2016.TS.XviD-VAiN
11	75.173.228.55	40361	µTorrent 3.4.7	06/18/2016 18:27:59	Criminal.2016.TS.XviD-VAiN
12	75.173.254.42	50085	µTorrent 3.4.7	06/18/2016 19:19:57	Criminal.2016.TS.XviD-VAiN
13	174.24.97.92	56876	µTorrent 3.4.7	06/18/2016 23:17:56	Criminal.2016.TS.XviD-VAiN

File Hash	ISP	Region	City	Province
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	Comcast Cable	Colorado	Littleton	Arapahoe County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County
SHA1: E6BB30EB8543BA90E894C9E8521C423CDD02B1F2	CenturyLink	Colorado	Colorado Springs	El Paso County