IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UN4 PRODUCTIONS, INC.,	)	
	)	
Plaintiff,	)	Case No.: 17-cv-4861
	)	
v.	)	
	)	Judge Matthew F. Kennelly
DOES 1-23,	)	
	)	
Defendants.	)	

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

I. Introduction

This copyright suit relates to the ongoing copyright infringement under the copyright laws of the United States (17 U.S.C. § 101 *et seq*.). In particular, this action seeks to address the infringement of Plaintiff's copyrighted mainstream motion picture entitled *Boyka Undisputed 4*, an action/crime/thriller directed by Todor Chapkanov, and stars Scott Adkins, Teodora Duhovnikova and Alon Aboutboul, among others. The Motion Picture has significant value and has been created and produced at considerable expense.

The illegal downloading of mainstream movies to avoid purchasing a theater ticket, buying a DVD or paying a rental fee is so pervasive that certain segments of the public appear to consider it acceptable. There are even websites devoted to illegal copying. One such website is *The Pirate Bay* which includes instructions on how to download the required pirating software, usually a torrent.[1] *The Pirate Bay* even provides a convenient "Pirate Search" function that enables infringers to "shop" for illegal copies of games, music, movies, books and software. This brazen and widely accepted scheme for illegal copying, which clearly is an intentional act since it requires an infringer to install special software and search out movies to pirate, is the problem addressed by this lawsuit.

Cloaked in the anonymity of the Internet, digital pirates banded together into swarms using file-sharing technology such as BitTorrent to illegally obtain and distribute high quality copies of the Motion Picture. While each single act of infringement may appear to be slight, collectively,

[1] THE PIRATE BAY, https://thepiratebay.org/ (last visited July 11, 2017) ("How do I download?").

illegal downloading often starts even before a movie is released and costs legitimate industries millions of dollars. Not only are movies pilfered, the pirates' other prizes include TV shows, computer games, e-books, software and music.

Thus, this suit not only represents a single copyright owner faced with the daunting task of protecting its property from the irreparable harm caused by thousands of swarming infringers, it is emblematic of the fight of the motion picture industry and other legitimate creative businesses that rely on copyright protection. Denying Plaintiff the discovery needed to pursue the infringing swarm in a single action endorses and encourages the ongoing infringement. It frees the pirates to roam the Internet searching for prizes by providing shelter through the anonymity of the Internet and the high cost of individual enforcement.

Plaintiff sued each Defendant as a "Doe" because Defendants committed infringement using on-line pseudonyms ("user names" or "network names"), not their true names. Plaintiff has only been able to identify the Doe Defendants by (1) their Internet Protocol ("IP") addresses, (2) the dates and times of the infringement, (3) the hash value which identifies each Defendant as participating in the same swarm and (4) the location of each IP address within Illinois.

Defendants' actual names can only be obtained 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 records kept in the regular course of business. Accordingly, Plaintiff seeks leave of Court to serve limited discovery prior to a Rule 26(f) conference on the non-party ISPs solely to determine the true identities of the Doe Defendants. Plaintiff requests that the Court enter an order allowing Plaintiff to serve Rule 45 subpoenas on the ISPs immediately and that the ISPs comply with the subpoenas.

The Mandatory Initial Discovery Pilot Project (MIDP) supersedes Rule 26(a)(1), and does not generally affect the grounds for or relief sought in this Motion. See Standing Order in MIDP Cases, UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS, http://www.ilnd.uscourts.gov/Pages.aspx?jYyawIFLXKMJrmXzxFk8lw== ("MIDP Standing Order"). Plaintiff is aware of and will of course follow the Northern District of Illinois's MIDP requirements, which are triggered by a responsive pleading. See MIDP Standing Order 3, § A(4) ("A party seeking affirmative relief must serve its responses to the mandatory initial discovery no later than 30 days after the first pleading filed in response to its complaint . . ."). Yet Plaintiff must first identify the Doe Defendants before a responsive pleading is possible.

Rule 26(d)(1) provides that a "party may not seek discovery from any source before the parties have conferred as required by Rule 26(f)." Fed. R. Civ. P. 26(d)(1). The Rule 26(f) conference triggers the time for parties to provide Rule 26(a) disclosures. Fed. R. Civ. P. 26(a)(1)(C). Likewise, the MIDP Standing Order provides that the "parties to this litigation are ordered to provide mandatory initial discovery responses as set forth in Section B before initiating any further discovery in this case." MIDP Standing Order 1, § A(1). However, under the MIDP Standing Order, a responsive pleading starts the clock on the MIDP disclosures, MIDP Standing Order 3, § A(4), not the Rule 26(f) conference. To the extent that the MIDP Standing Order imposes limitations on discovery separate from and in addition to the timing restrictions of Rule 26(d)(1), Plaintiff requests that the Court grant leave to conduct discovery prior to the Rule 26(f) conference and prior to the MIDP disclosures.[2]

If the Court grants this Motion, Plaintiff will serve subpoenas on the ISPs requesting limited identifying information (name and current address only). 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

Pursuant to Rule 26(d)(1), except for circumstances not applicable here, a party may not propound discovery in advance of a Rule 26(f) conference absent a court order. Rule 26(b) provides courts with the authority to issue such an order: "[f]or good cause, the court may order discovery of any matter relevant to the subject matter involved in the action." In Internet infringement cases, courts routinely find good cause exists to issue a Rule 45 subpoena to discover a Doe defendant's identity, prior to a Rule 26(f) conference, where: (1) plaintiff makes a prima facie showing of a claim of copyright infringement, (2) plaintiff submits a specific discovery request, (3) there is an absence of alternative means to obtain the subpoenaed information, (4)

[2] Indeed, Plaintiff would be unable to comply with the MIDP Standing Order's requirements (which in any event are not yet triggered) until Plaintiff has the identifying information it hereby requests.

there is a central need for the subpoenaed information, and (5) defendants have a minimal expectation of privacy. See Arista Records, LLC v. Doe 3, 604 F.3d 110 (2d Cir. 2010) (citing to Sony Music Entm't v. Does 1-40, 326 F.Supp.2d 556, 564-65 (S.D.N.Y. 2004)); BMG Music v. Doe #4, No. 08-cv-135, 2009 WL 2244108, at *3 (M.D.N.C. July 24, 2009); Elektra Entm't Group, Inc. v. Doe, No. 08-cv-115, 2008 WL 5111886, at *4 (E.D.N.C. Dec. 4, 2008); Warner Bros. Records, Inc. v. Doe, No. 08-cv-116, 2008 WL 5111883, at *4 (E.D.N.C. Dec 4, 2008); see also Arista Records LLC v. Does 1-19, 551 F.Supp.2d 1, 6-7 (D.D.C. 2008) (noting that in the "overwhelming" number of cases where copyright infringement plaintiffs sought to identify "Doe" defendants, courts "routinely applied" the good cause standard to permit discovery). Here, all of the good cause elements are present. Thus, Plaintiff respectfully submits that this Court should grant the Motion.

A. Precedent Allowing Discovery to Identify Doe Defendants

In copyright cases brought by motion picture studios and record companies against Doe defendants, this Court and other courts have granted 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. Warner Bros. Records, Inc. v. Does 1-6, 527 F.Supp.2d 1, 2 (D.D.C. 2007) (allowing plaintiffs to serve a Rule 45 subpoena upon Georgetown University to obtain the true identity of each Doe defendant, including each defendant's true name, current and permanent addresses and telephone numbers, email address, and Media Access Control ("MAC") address) (citing Memorandum Opinion and Order, UMG Recordings, Inc. v. Does 1-199, No. 04-093(CKK) (D.D.C. March 10, 2004); Order, UMG Recordings v. Does 1-4, 64 Fed. R. Serv. 3d (Callaghan) 305 (N.D. Cal. March 6, 2006)).

In fact, for the past few years, federal district courts throughout the country, including Courts in the Northern District of Illinois, have granted expedited discovery in Doe Defendant lawsuits that are factually similar to the present lawsuit.[3] In these cited cases and others like them,

[3] Representative cases include Countryman Nevada, LLC v. Does 1-46, No. 14-cv-1381, 2014 WL 4947587 (N.D. Ill. Sept. 30, 2014) (Darrah, J.); SITE B v. Does 1-51, No. 13-cv-5295, 2014 WL 902688 (N.D. Ill. Mar. 7, 2014) (Leinenweber, J.); TCYK, LLC v. Does 1-44, No. 13-cv-3825, 2014 WL 656786 (N.D. Ill. Feb. 20, 2014) (Dow, J.); Bicycle Peddler, LLC v. Does 1-99, No. 13-cv-2375, 2013 WL 4080196 (N.D. Ill. Aug. 13, 2013) (Gottschall, J.); reFX Audio Software, Inc. v. Does 1-111, No. 13-cv-1795, 2013 WL 3867656 (N.D. Ill. July 23, 2013) (Gettleman, J.); TCYK, LLC v. Does 1-87, No. 13-cv-3845, 2013 WL 3465186 (N.D. Ill. July 10, 2013) (Tharp, J.); Bicycle Peddler, LLC v. Does 1-12, 295 F.R.D. 274, 276 (N.D. Ill. 2013) (Tharp, J.); Pacific Century Int'l v. Does 1-25, No. 12-cv-1535 (N.D. Ill. June 28, 2012) (Bucklo, J.); Hard Drive Productions

copyright holder plaintiffs have obtained the identities of P2P network users from ISPs through expedited discovery using information similar to that gathered by Plaintiff in the present case, and they have used that information as the basis for their proposed subpoenas to these ISPs. In this case, Plaintiff is only seeking the name and current address of each Doe Defendant.

The following factors are considered 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, at *1-2, (N.D. Cal. 2003).

B. Good Cause Exists to Grant the Motion

1. Plaintiff has a Prima Facie Claim for Copyright Infringement

a. Overview of Allegations and Factual Showings

The Complaint alleges that 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 available for distribution to others the copyrighted Motion Picture for which Plaintiff holds the exclusive reproduction and distribution rights. Compl. ¶¶ 12-16. Maverickeye UG ("MEU"), a provider of online anti-piracy services for the motion picture industry, was engaged to monitor this infringing activity. Declaration of Daniel Arheidt (attached as Exhibit A).

An IP address is a unique numerical identifier that is automatically assigned to an Internet user by the user's Internet Service Provider ("ISP"). In logs kept in the ordinary course of business, ISPs 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. Arheidt Decl. ¶ 17.

Only the ISP to which a particular IP address has been assigned for use by its subscribers

---

v. Does 1-48, No. 11-cv-9062, 2012 WL 2196038 (N.D. Ill. June 14, 2012) (Kim, J.); Pacific Century Int'l v. Does 1-31, No. 11-cv-9064, 2012 WL 2129003 (N.D. Ill. June 12, 2012) (Leinenweber, J.); First Time Videos, LLC v. Does 1-76, 276 F.R.D. 254, 255 (N.D. Ill. 2011) (Bucklo, J.).

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. Id. at ¶ 18. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

To identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted Motion Picture, Daniel Arheidt, a software consultant with MEU, was responsible for analyzing, reviewing and attesting to the results of the investigation.

MEU used forensic software to scan peer-to-peer networks for the presence of infringing transactions, id. at ¶ 23, and Arheidt isolated the transactions and the IP addresses of the users responsible for copying and distributing the Motion Picture. Id. at ¶ 24. Through each of the transactions, the computers using the IP addresses identified in Exhibit B of the Complaint transmitted a copy or a part of a copy of a digital media file identified by the relevant hash value. The IP addresses, hash values, dates and times contained in 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 work. Id. at ¶ 25.

Moreover, the users were sharing the exact same copy of the Motion Picture. Id. at ¶ 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. Using a hash tag to identify different copies of the Motion Picture, it was confirmed that these users reproduced the very same copy of the Motion Picture. Id.

The MEU 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. Id. at ¶ 27.

The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Complaint Exhibit B were located in Illinois. Id. at ¶ 28. Although an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet connection used for the transaction. Id. 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 databases by ISPs. Id.

As set forth in Complaint Exhibit B, it was confirmed not only that the users distributed the files in Illinois, but also the specific location where the distribution took place.

The targeted period of the swarm in this matter covers a one-day period, April 8, 2017. Torrent swarms can survive over extended periods of time (months or years) and provide users with exactly the same file comprising exactly the same pieces. A primary factor determining the size of a swarm is the popularity of the product that the file contains (movie, audio, TV series, etc.). For example, a recently released movie can lose popularity within weeks or months, whereas a famous album of a rock band might continue to be popular for several years.

It is not necessary for each of the Defendants to have directly interacted with each other Defendant, or to have shared a piece of the file with each and every Defendant when downloading the movie. The Defendants are properly joined because their actions directly relate back to the same initial seed of the swarm, and their alleged infringement further advanced the series of infringements that began with the initial seed and continued through other infringers. In doing so, the Defendants all acted under the same system. It is sufficient that the Defendants shared pieces that originated from the same (identical) file, and opened their computer to allow others to connect and receive those pieces. See, e.g., Patrick Collins, Inc. v. John Does 1-21, 11-cv-15232, 2012 WL 1190840, at *7-8 (E.D. Mich. Apr. 5, 2012) (attached as Exhibit B).

The question of whether defendants' actions in a swarm justified joinder under Rule 20 arose in TCYK, LLC v. Does 1-44, 13-cv-3825, 2014 WL 656786 (N.D. Ill. Feb. 20, 2014) (Dow, J.) (attached as Exhibit C). In a well-reasoned opinion, not only did the District Court conclude that they did, but also noted that this viewpoint is starting to be adopted widely in the Northern District of Illinois.

> The Court acknowledges the strong arguments on both sides of the issue, but agrees with the weight of the authority and growing trend in this district that participation in a swarm qualifies as engaging in a "series of transactions or occurrences" for the purpose of Rule 20. As other judges in this district have

> concluded, a user who connects to a swarm joins a "cooperative endeavor." *TCYK, LLC,* 2013 WL 3465186 at *1. Regardless of whether these forty-four defendants contemporaneously participated in the swarm, shared bits of the seed file with each other, or even shared bits of the file at all, each joined the swarm knowing that his participation increased the swarm's ability to disseminate a common seed file quickly and efficiently. The Court therefore concludes that a logical relationship exists among the actions of the Defendants such that joinder is proper. Moreover, joinder here serves the interest of judicial economy, which underlies Rule 20. Wright *et al., supra,* § 1653. "At the pleading stage, it is more efficient to join Doe Defendants in one action than to require separate lawsuits. Individual litigations, at least at the early stages of litigation, would be needlessly expensive for both [Plaintiff] and the courts and would frustrate the judicial efficiency policies at the heart of Rule 20." *Malibu Media,* 291 F.R.D. at 204-05.

TCYK, LLC, 2014 WL 656786, at *3.

While not binding on this Court, TCYK, LLC stands as persuasive authority for the view that the cooperative and interdependent actions of defendants participating in a swarm constitute the requisite "series of transactions or occurences" under Rule 20 to justify joining them in common litigation involving the downloading of the motion picture at issue.

b. Plaintiff's Prima Facie Showing of Copyright Infringement

Plaintiff has sufficiently identified the Doe Defendants through the unique IP address that each Doe Defendant was assigned at the time of the unauthorized distribution and copying of the copyrighted Motion Picture. 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.

A prima facie claim of copyright infringement consists of two elements: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original. Feist Publ'ns. Inc. v. Rural Tele. Serv. Co., Inc., 499 U.S. 340, 361 (1991). Plaintiff satisfied the first good cause factor by properly pleading a cause of action for copyright infringement. Compl. ¶¶ 12-16; see also 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 . . ."); Elektra,

2008 WL 5111886, at *4 ("[P]laintiffs have established a prima facie claim for copyright infringement, as they have sufficiently alleged both ownership of a valid copyright and encroachment upon at least one of the exclusive rights afforded by copyright."); Warner Bros. Records, Inc. v. Doe, No. 08-cv-116, 2008 WL 5111883, at *4 (E.D.N.C. Dec. 4, 2008) (same). Accordingly, Plaintiff has met and exceeded its obligation to plead a prima facie case.

2. Plaintiff Seeks Limited and Specific Discovery

Plaintiff only seeks to discover the name and current address of each Defendant. This is all specific information that is in the possession of each Defendant's ISP that will enable Plaintiff to serve process. Since the requested discovery is limited and specific, Plaintiff has satisfied the second good cause factor.

3. No Alternative Means Exist to Obtain Defendant's True Identities

Other than receiving the information from the Defendants' ISP, there is no way to obtain Defendants' true identity because the ISP is the only party who possesses records which track IP address assignment to their subscribers. Consequently, the ISP is the source for information relating to associating an IP address to a real person. Since there is no other way for Plaintiff to obtain Defendant's identity, except by serving a subpoena on Defendant's ISPs demanding it, Plaintiff has established the third good cause factor. See Columbia, 185 F.R.D. at 578-80; Elektra, 2008 WL 5111886, at *4 (finding that the feasibility of a suggested alternative method of determining defendants' identities by hiring a private investigator to observe downloading "is questionable at best"); Warner Bros., 2008 WL 5111883, at *4 (same).

4. Discovery is Needed to Advance the Asserted Claims

Plaintiff will not be able to serve the Defendants with process and proceed with this case without the requested discovery. Plaintiff's statutorily protected property rights, in which millions have been invested, are at issue in this suit and, therefore, the equities should weigh heavily in favor of preserving Plaintiff's rights. Since identifying the Defendant by name is necessary for Plaintiff to advance the asserted claims, Plaintiff has established the fourth good cause factor. See BMG Music, 2009 WL 2244108, at *3 (finding under nearly identical circumstances that "[p]laintiffs have shown that the subpoenaed information - Doe #4's identity – is centrally needed

to advance Plaintiff's copyright infringement claim"); Sony, 326 F.Supp at 566.

5. Plaintiff's Interest in Knowing Defendants' True Identities Outweighs Defendants' Interests in Remaining Anonymous

Plaintiff has a strong legitimate interest in protecting its copyright. Defendants are copyright infringers with no legitimate expectation of privacy in the subscriber information provided to the ISP, much less in distributing the copyrighted work in question without permission. See 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"); BMG Music, 2009 WL 2244108, at *3 (finding under nearly identical circumstances that "[p]laintiffs have shown that Defendant Doe #4 has a minimal expectation of privacy downloading and distributing copyrighted songs without permission"); 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); Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 8-9 (D.D.C. Apr. 28, 2008) (finding that the "speech" at issue was the 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"); Arista Records, LLC v. Doe No. 1, 254 F.R.D. 480, 481 (E.D.N.C. 2008); Sony, 326 F.Supp.2d at 566 ("defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission"); U.S. v. Hambrick, 55 F.Supp.2d 504, 508 (W.D. Va. 1999), aff'd, 225 F.3d 656 (4th Cir. 2000).

Downloading a mainstream motion picture is no different than downloading a song. Being named as a defendant in this action does not expose an individual to embarrassment. It is not blackmail. In fact, copying music and mainstream movies is so pervasive that certain segments of the public apparently accept it without question. This is the specific problem this lawsuit addresses – copying a mainstream movie is no different than downloading a song, it raises no privacy concerns.

C. Irreparable Harm Establishes Good Cause to Grant the Motion

Good cause exists here for the additional reason that a claim for copyright infringement presumes irreparable harm to the copyright owner. This is especially true in this matter since the copying results in lost ticket sales, and will also erode rentals and purchases. See Elvis Presley Enter., Inc. v. Passport Video, 349 F.3d 622, 631 (9th Cir. 2003); UMG Recordings, Inc. v. Doe, 2008 WL 4104214 (N.D. Cal. 2008) (finding good cause for expedited discovery exists in Internet infringement causes, 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); see also Melville B. Nimmer & David Nimmer, Nimmer on Copyright, § 14.06[A], at 14-03 (2003).

The first and necessary step that Plaintiff must take to stop the infringement of its valuable copyright 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 this case forward." Semitool, Inc. v. Tokyo Electron Am., Inc., 208 F.R.D. 273, 277 (N.D. Cal. 2002).

III. Conclusion

For the foregoing reasons, Plaintiff respectfully requests the Court to grant the pending Motion for Leave to Take Discovery Prior to the Rule 26 Conference. Plaintiff requests permission to serve a Rule 45 subpoena on the ISPs it has identified as of this date, and those it identifies in the future, so that the ISPs can disclose the name and current address of each Doe Defendant that Plaintiff has identified to date, 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,

Dated: July 14, 2017

UN4 PRODUCTIONS, INC.

By: s/Michael A. Hierl

Michael A. Hierl (Bar No. 3128021)
Todd Pierce-Ryan (Bar No. 6321299)
Hughes Socol Piers Resnick & Dym, Ltd.
70 W. Madison Street, Suite 4000
Chicago, Illinois 60602
(312) 580-0100 Telephone
(312) 580-1994 Facsimile

Attorneys for Plaintiff
UN4 Productions, Inc.

CERTIFICATE OF SERVICE

The undersigned attorney hereby certifies that a true and correct copy of the foregoing Memorandum in Support of Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) conference was filed electronically with the Clerk of the Court and served on all counsel of record and interested parties via the CM/ECF system on July 14, 2017.

s/Michael A. Hierl

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UN4 PRODUCTIONS, INC.,	)	
	)	
Plaintiff,	)	Case No.: 17-cv-4861
	)	
v.	)	
	)	Judge Matthew F. Kennelly
DOES 1-23,	)	
	)	
Defendants.	)	

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

1. My name is Daniel Arheidt. 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 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 which Maverickeye UG monitored for Plaintiff's Motion Picture (*Boyka Undisputed 4*) 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 which 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 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 copyrighted 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 peer.

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 logs of the intermediaries 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 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, Maverickeye UG (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine whether or not a particular motion picture is copied in the downloaded file, but also confirms the copying by a visual comparison of the downloaded file and the Motion Picture.

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 identifies the Doe Defendants and downloads the motion pictures they were distributing, Maverickeye UG opens the downloaded files, watches them and confirms that they contain 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, 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 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 single "swarm" of

users who were reproducing, distributing, displaying or performing the copyrighted Motion Picture on April 8, 2017.

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 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 investigation. The location of each IP address is set forth in Complaint Exhibit B. 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.

29. I acknowledge that there were other swarms, employing different "seed files," through which others copied and distributed Plaintiff's copyrighted Motion Picture before, during and after the timeframe referenced in Paragraph 25 above. Plaintiff, however, has limited the pool of Defendants in this lawsuit only to those who downloaded the movie from a single seed file in a brief and definite temporal period, specifically with the intent to prosecute an action only against defendants who were involved in the same transaction, occurrence, or series of transactions or occurrences.

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 7 day of July 2017.

By: _____
Daniel Arheidt

EXHIBIT B

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

PATRICK COLLINS, INC.,

Plaintiff,

v.

JOHN DOES 1-21,

Defendants.
_____/

CIVIL ACTION NO. 11-15232

DISTRICT JUDGE DENISE PAGE HOOD

MAGISTRATE JUDGE MARK A. RANDON

REPORT AND RECOMMENDATION TO DENY DEFENDANT JOHN DOE 18'S MOTION TO QUASH SUBPOENA AND TO DISMISS (DKT. NO. 6)

I. INTRODUCTION

Patrick Collins, Inc. ("Plaintiff") is the registered copyright owner of the adult movie "Cuties 2" (the "Movie" or "Work"). Plaintiff brought suit against 21 John Doe Defendants (collectively, "Defendants") alleging direct and contributory copyright infringement of the Movie. Plaintiff claims that Defendants downloaded and uploaded the Movie via a peer-to-peer protocol, BitTorrent. On December 16, 2011, this Magistrate Judge granted Plaintiff's motion for leave to serve third party subpoenas on Defendants' Internet Service Providers ("ISPs") to obtain Defendants' names and residential addresses (Dkt. No. 5).[1]

John Doe 18 ("Doe 18") was among those Defendants whose names and addresses Plaintiff sought. Doe 18 moves to quash the subpoena served on his/her ISP and to dismiss Plaintiff's claims due to misjoinder (Dkt. No. 6). Judge Denise Page Hood referred the motion

[1] Currently, Defendants can only be identified by their Internet Protocol ("IP") addresses. "A party may not seek discovery from any source before the parties have conferred as required by rule 26(f), except . . . when authorized . . . by court order." Fed R. Civ. P. 26(d)(1).

to this Magistrate Judge for a report and recommendation (Dkt. No. 4). The issues have been fully briefed (Dkt. Nos. 6, 9); oral argument was held on March 8, 2012.

The facts of this case are complex and highly technical, involving concepts of computer science, networking, and other technology. Despite this complexity, the straightforward and well-established permissive joinder rule governs the outcome. Because this Magistrate Judge finds that joinder is proper, **IT IS RECOMMENDED** that Doe 18's motion to quash the subpoena and dismiss be **DENIED**.

II. FACTUAL BACKGROUND

Before delving into the workings of BitTorrent,[2] a simplified overview of Plaintiff's claims may be helpful:

Plaintiff alleges that a specific individual received the Movie "Cuties 2," used a computer to break the Movie down into small pieces, and created a file that allowed the pieces of the Movie to be downloaded over the internet (Dkt. No. 1; Compl.). According to Plaintiff, each Defendant uploaded and downloaded pieces of the Movie through a series of transactions that can be traced back to this specific individual, known as the "Initial Seeder." Everyone who can be traced back to this Initial Seeder is part of a common group of users ("Swarm") downloading or uploading pieces of the Movie. BitTorrent is the protocol that allowed Defendants to engage in their allegedly related transactions. Plaintiff alleges that Defendants are part of the same Swarm, and this makes them ripe for Joinder under Federal Rule of Civil Procedure 20.

[2] This Spring, I had the good fortune to have an exceptionally bright law student, Matthew Crist, as an intern. Before attending law school Matt was a computer technician. His skill in explaining the technology to the technologically challenged and assistance with this report and recommendation were invaluable.

Plaintiff chose to sue 21 potential defendants in the Swarm.[3] Besides being in the same Swarm and copying the Movie, Plaintiff alleges that Defendants reside in the Eastern District of Michigan (based on their IP addresses).[4]

A. How BitTorrent Works: A Detailed Explanation

For the technologically challenged, a working definition of a few recurring terms is useful to understand how BitTorrent operates:

Glossary of Terms

Communication Protocol: Procedures that enable devices within a computer network to exchange information. Also known as a protocol. *McGraw-Hill Dictionary of Scientific and Technical Terms* 440 (6th ed. 2003).

Hash Identifier: A way to uniquely identify an encoded file. There are many variations on this concept, however, it is simply a long string of letters and numbers that form a unique string. It is practically impossible for two Hash Identifiers to be identical because of the extremely long string that is randomly generated for each piece when the Torrent is made.

Hypertext Transfer Protocol (HTTP): Another system of communication standards. HTTP is the protocol by which websites on the World Wide Web communicate with browsers; hence the HTTP before a website's address.

File: A collection of related records treated as a unit. *McGraw-Hill Dictionary of Scientific and Technical Terms* 797 (6th ed. 2003). A file can be a movie, a set of text, a picture, *et cetera*. The computer science use of the term is analogous to the term "file" in common parlance.

File Transfer Protocol (FTP): Another system of communication standards wherein a file is directly transferred from the server to the downloader.

Internet Protocol (IP): The set of standards responsible for ensuring that data packets transmitted over the Internet are routed to their intended destinations. *McGraw-Hill Dictionary of Scientific and Technical Terms* 1101 (6th ed. 2003).

---

[3] Plaintiff is not required to join all parties under the permissive joinder rule. Nor may Defendants demand that Plaintiff join another potential defendant that is not a "necessary party." *See, Field v. Volkswagenwerk AG*, 626 F.2d 293, 299 (3d Cir. 1980).

[4] The court must have personal jurisdiction and venue must be proper to consider the issue of joinder. Plaintiff has satisfied these conditions.

IP Address: The numeric representation of a device on a network that communicates using Internet Protocol. The address is of the form "xxx.xxx.xxx.xxx."

Leecher: (1) A BitTorrent user who has not yet fully downloaded a file; (2) A user who has inhibited, or throttled, the upload speed setting in the Client Program so that it will download much more than upload; (3) A user who exits BitTorrent after the download is complete to prevent uploading to other peers.

Piece: An initial seeder breaks a file into pieces. The pieces are typically one-quarter megabyte in size; however, the last piece will be the size of the remainder. The Hash of the pieces is included in the Torrent file. At any given moment, a peer may be simultaneously uploading and downloading pieces from and to many different peers within the same swarm for the same Torrent. Bram Cohen, *Incentives Build Robustness in BitTorrent*, 1 (May 22, 2003), http://bittorrent.org/bittorentecon.pdf.

Seeder: A user who has downloaded the whole file and is uploading all of its pieces to other peers in the swarm. Cohen, *Incentives Build Robustness in BitTorrent, supra.*

Seeder, Initial: The individual who has taken a complete file (a movie, picture, program, or any other kind of computer file) broken it down into pieces, encoded it with Hashes, created the Torrent file with the data about that file and its tracker, and made the complete file available on BitTorrent.

When users begin downloading from this initial seeder, a swarm is created; each individual in the first stage of the swarm downloads the same file from the same initial seeder with the same Hashes and then the file spreads virally with that same digital fingerprint as torrent

Swarm: A group of users downloading the desired file from each other, from seeders (if any are online), and from the initial seeder (if still online). Additionally, a swarm denotes that all of the users in it are downloading files with the same Hash Identifier.

Uniform Resource Locator (URL): The unique Internet address assigned to a Web document or resource by which it can be accessed by all Web browsers. The first part of the address specifies the applicable Internet protocol, for example, http or ftp; the second part provides the IP address or domain name of the location. Abbreviated "URL." *McGraw-Hill Dictionary of Scientific and Technical Terms* 2225 (6th ed. 2003).

1. BitTorrent defined

> BitTorrent is a protocol for distributing files. It identifies content by URL and is designed to integrate seamlessly with the web. Its advantage over plain HTTP is that when multiple downloads of the same file happen concurrently, the downloaders upload to each other, making it possible for the file source to support very large numbers of downloaders with only a modest increase in its load.

See Bram Cohen, *The BitTorrent Protocol Specification*, BitTorrent.org (Feb. 28, 2008), http://www.bittorrent.org/beps/bep_0003.html. Users of the BitTorrent protocol download and install the BitTorrent program ("Client Program" or "Client") onto their computers and then search the internet for a unique ".torrent"[5] file ("Torrent"). *See* Cohen, *The BitTorrent Protocol Specification, supra*. After downloading the relatively small Torrent, the Torrent directs the Client Program to the location and identity of the pieces of the desired file (or Work) by way of a tracker. Cohen, *The BitTorrent Protocol Specification, supra*; *e.g.*, Cohen, *Incentives Build Robustness in BitTorrent, supra*. The Client Program then downloads the pieces of the file from other BitTorrent users and stores them locally on the user's computer. *See* Cohen, *Incentives Build Robustness in BitTorrent, supra*.

2. The Torrent File

The Torrent file is the hub of the BitTorrent system. The Torrent file is created by the initial seeder. *See* Cohen, *The BitTorrent Protocol Specification, supra*. The Torrent file contains: the URL of the tracker, information about the file that has been broken down into pieces, the number and size of the pieces, and the SHA1 hashes ("Hash Identifier") unique to each initial seeder's Torrent file. Cohen, *The BitTorrent Protocol Specification, supra*. When the initial seeder breaks the file (here, the copyrighted Movie) into pieces, each piece gets encoded using a Hash Identifier. Cohen, *The BitTorrent Protocol Specification, supra*. After a user has downloaded all of the pieces of the desired file from peers, the file will be reconstituted

[5] To be explained in more detail below.

into a complete copy of the original file and will be usable just as the original. As a movie, it will then be viewable.

3. The Hash Identifier

The Unique Hash Identifier (also known as a hash tag, SHA1 hash, or a digital fingerprint) is a long string of letters and numbers[6] that is used to compare a copy of a file with the original to ensure data integrity. In the context of BitTorrent, the Hash Identifier is randomly generated and assigned to each piece of a file when the initial seeder creates the Torrent file. This Torrent is then downloaded by users who wish to obtain the work that the initial seeder has made available. Before two peers can transact a piece of the Work, BitTorrent compares the Hash of each user. If the Hash Identifiers are not identical, the connection between peers is severed and no transaction takes place. Cohen, *The BitTorrent Protocol Specification*, *supra*.

4. The Peers

Users who download and open the same Torrent file are coordinated by the tracker. Cohen, *Incentives Build Robustness in BitTorrent*, *supra*. Unless the user affirmatively inhibits uploading, the Client Program will announce and automatically upload each piece to other peers who have used the same Torrent. Cohen, *Incentives Build Robustness in BitTorrent*, *supra*. If the user has downloaded all of the pieces, he will automatically become a seeder and will automatically upload the file to all peers in the swarm as they request pieces.[7] This coordination through the Torrent file is key to the success of a swarm, because each individual user's success or failure to fully download the file is dependent on other users downloading the same Torrent

[6] Plaintiff alleges that each Defendant downloaded a piece of the Movie with the exact same Hash Identifier: EE7B1E84B6FD741359D99A0397DF043842BAB4D7. (Dkt. No. 1 at 9).

[7] The desire of the creator of BitTorrent is that users become seeders instead of inhibiting the upload of pieces to other users (leeching); thus, the default setting is that each user automatically uploads each piece to other peers at all times until the user affirmatively chooses to disable uploading, exits the program or deletes the Torrent. *See* Cohen, *Incentives Build Robustness in BitTorrent*, *supra*. The fact that Plaintiff's investigator was able to download a piece from each Defendant means that they did not inhibit uploading.

file and allowing the upload of pieces. *See* Cohen, *Incentives Build Robustness in BitTorrent*, *supra*; *see e.g.*, Cohen, *The BitTorrent Protocol Specification*, *supra*.

III. FACTUAL ANALYSIS

A. Steps Taken By Plaintiff's Investigator

Plaintiff alleges that its investigator ("IPP") was able to download at least one piece of the copyrighted Movie from each Defendant (Dkt. No. 1 at 8-10). It is important to understand the implications of this allegation before determining whether joinder is proper. If IPP downloaded a piece of Plaintiff's copyrighted Movie from each Defendant (and, conversely, each Defendant uploaded at least one piece of the Movie to IPP) then each Defendant had at least one piece of the Movie -- traceable via Hash Identifier to the same Initial Seeder -- on his or her computer and allowed other peers to download pieces of the Movie.

By way of illustration: IPP's computer connected with a tracker, got the IP address of each of Defendants' computers, connected with each Defendants' computer, and downloaded at least one piece of the Movie from each Defendants' computer. During this transaction, IPP's computer verified that each Defendants' piece of the Movie had the expected Hash;[8] otherwise, the download would not have occurred.

If Plaintiff's allegations are true, each Defendant must have downloaded the piece(s) each had on his or her computer in one, or more, of the following four ways:

1) the Defendant connected to and transferred a piece of the Movie **from the initial seeder**; or

2) the Defendant connected to and transferred a piece of the Movie **from a seeder** who downloaded the completed file from the initial seeder or from other peers; or

3) the Defendant connected to and transferred a piece of the Movie **from other Defendants** who downloaded from the initial seeder or from other peers; or

[8] The Hash value of EE7B1E84B6FD741359D99A0397DF043842BAB4D7. (Dkt. No. 1 at 9).

4) the Defendant connected to and transferred a piece of the Movie **from other peers** who downloaded from other Defendants, other peers, other Seeders, or the Initial Seeder.

In other words, in the universe of possible transactions, at some point, each Defendant downloaded a piece of the Movie, which had been transferred through a series of uploads and downloads from the Initial Seeder, through other users or directly, to each Defendant, and finally to IPP.

Therefore, each Defendant is logically related to every other Defendant because they were all part of a series of transactions linked to a unique Initial Seeder and to each other. This relatedness arises not merely because of their common use of the BitTorrent protocol, but because each Defendant affirmatively chose to download the same Torrent file that was created by the same initial seeder, intending to: 1) utilize other users' computers to download pieces of the same Movie, and 2) allow his or her own computer to be used in the infringement by other peers and Defendants in the same swarm.

IV. LEGAL ANALYSIS

At the outset, it should be noted that Doe 18's "motion to quash subpoena and dismiss," must be construed as a motion to quash and motion *to sever*. Severance – not dismissal – is the correct remedy of misjoinder. *See* Fed. R. Civ. P. 21 ("Misjoinder of parties is not ground for dismissing an action. On motion or on its own, the court may at any time, on just terms, add or drop a party. The court may also sever any claim against a party"); *see also*, *Call of the Wild Movie, LLC v. Does 1-1,062*, 770 F.Supp.2d 332, 342 (D.D.C. 2011) (clarifying that while misjoinder is not fully defined, if it is found, severance is the correct remedy); *Disparte v. Corporate Executive Board*, 223 F.R.D. 7, 12 (D.D.C. 2004) (stating that if the preconditions of Rule 20(a) are not satisfied, then the misjoined parties are to be severed into discrete actions);

e.g., Donkeyball Movie, LLC., Does 1-171, 810 F.Supp.2d 20, 27 n.6 (D.D.C. 2011); *Hard Drive Productions v. Does 1-188*, 809 F.Supp.2d 1150, 1165 (N.D. Ca. 2011).[9]

A. **Permissive Joinder**

Federal Rule of Civil Procedure 20(a)(2) allows the joinder of defendants if:

> (A) any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence or series of transactions or occurrences; and
>
> (B) any question of law or fact common to all defendants will arise in the action.

Fed. R. Civ. P. 20(a)(2). Rule 20(a)(2) lists three categories of rights to relief and supplies two preconditions to joinder. To satisfy Rule 20(a)(2), a plaintiff must assert a right to relief against a group of defendants jointly, severally, or in the alternative.[10] The preconditions are: 1) the right to relief must be with respect to or arising out of the same transaction, occurrence or series of transactions or occurrences; and 2) at least one question of law or fact must be common to all defendants.

Rule 20 should be viewed in light of the overarching policy of Rule 1 which requires that the rules "be construed and administered to secure the *just, speedy, and inexpensive* determination of every action and proceeding." Fed. R. Civ. P. 1 (emphasis added). "The purpose of [Rule 20] is to promote trial convenience and expedite the final determination of disputes, thereby preventing multiple lawsuits. Single trials generally tend to lessen the delay, expense and inconvenience to all concerned." *Mosley v. General Motors Co.*, 497 F.2d 1330,

---

[9] If the Plaintiff is required to proceed against each of the 21 defendants separately, then the court would have to create 21 dockets and schedule 21 pre-trial conferences. After all that, the court may very well consolidate the 21 actions under Fed. R. Civ. P. 42; meanwhile, the Plaintiff and the court would have expended a great deal of time and money.

[10] A right to relief against defendants jointly requires concerted action by two or more parties. A right to relief severally against defendants means that each right to relief is separate and distinct from defendant to defendant and no interaction among the defendants is required. An 'alternative' right to relief may be asserted when plaintiff knows one of the defendants is liable, but does not know which one. 4 Moore's Federal Practice § 20.03. Plaintiff asserts a right to relief against Defendants jointly and a right to relief severally; however, a right to relief against the Defendants severally alone is sufficient to satisfy the first clause of Rule 20.

1332 (8th Cir. 1974) (citation omitted). Accordingly, the Supreme Court emphasized that, "[u]nder the Rules, the impulse is toward entertaining the broadest possible scope of action consistent with fairness to the parties; joinder of claims, parties and remedies is strongly encouraged." *United Mine Workers of America v. Gibbs*, 383 U.S. 715, 724, 86 S.Ct. 1130, 1138, 16 L.Ed.2d 218 (1966) (internal footnote omitted).

"In order to satisfy the first prong of [Rule 20], the claims must be logically related." *Disparte v. Corporate Executive Board*, 223 F.R.D. 7, 10 (D.D.C. 2004) (citing *Moore v. New York Cotton Exchange*, 270 U.S. 593, 610 (1926)). "The logical relationship test is flexible." *Disparte*, 223 F.R.D. at 10.

Furthermore, permissive joinder is to be liberally construed. *See Swan v. Ray*, 293 F.3d 1252, 1253 (11th Cir. 2002). Applying this liberal construction standard in *United States v. Mississippi*, 380 U.S. 128, 142, 85 S.Ct. 808, 13 L.Ed.2d 717 (1965), the Supreme Court found that allegations of a state-wide system designed to enforce the voter registration laws in a way that would inevitably deprive African-Americans of the right to vote solely because of their color, justified the joinder of registrars of six counties as defendants. The Supreme Court reversed a district court's decision which held that, "the complaint improperly attempted to hold the six county registrars jointly liable for what amounted to nothing more than individual torts committed by them separately with reference to separate applicants." *Mississippi*, 380 U.S. at 142. Although the district court's decision amounted to a finding of a lack of concerted action by the six registrars – who were from different geographical areas, acted independently of each other, and perhaps had never met one another – the Supreme Court interpreted Rule 20 to encompass a right to relief severally so long as transactional relatedness and commonality in fact or law are met. *Mississippi*, 380 U.S. at 142-43.

The permissive joinder of defendants is also encouraged for purposes of judicial efficiency. *See United Mine Workers of America,* 383 U.S. 715 at 724; *Disparte v. Corporate Executive Board*, 223 F.R.D. 7, 10 (D.D.C. 2004); *Donkeyball Movie, LLC., v. Does 1-171*, 810 F.Supp.2d 20, 26 n.6 (D.D.C. 2011); *but cf Hard Drive Productions v. Does 1-188*, 809 F.Supp.2d 1150, 1165 (N.D. Cal. 2011) (holding that filing 188 individual actions does not hinder plaintiff's ability to protect its copyright and that fairness to the defendants is more persuasive than judicial economy and fairness to the plaintiff).

1. Meaning of transaction

The Eighth Circuit clarified the meaning of the word "transaction" for purposes of Rule 20. *Mosley v. General Motors Co.*, 497 F.2d 1330, 1333 (8th Cir. 1974). "'Transaction' is a word of flexible meaning. It may comprehend a series of many occurrences, depending not so much upon the immediateness of their connection as upon their logical relationship." *Mosley v. General Motors Co.*, 497 F.2d 1330, 1333 (8th Cir. 1974) (citing *Moore v. New York Cotton Exchange*, 270 U.S. 593 46 S.Ct. 367 (1926)). Therefore, "Rule 20 would permit all reasonably related claims for relief by or against different parties to be tried in a single proceeding. *Absolute identity of all events is unnecessary.*" *Mosley*, 497 F.2d 1333 (emphasis added).

B. Joinder Is Proper

Applying the legal standards discussed above, joinder of Defendants is proper. Plaintiff alleges a right to relief severally against Defendants for direct and contributory copyright infringement of the Work; Plaintiff says that Defendants networked with other each other and/or with other peers through a series of transactions in the same swarm to infringe on Plaintiff's copyright. Stated simply:

> [I]t is difficult to see how the sharing and downloading activity alleged in the Complaint – a series of individuals connecting either directly with each other or

> as part of a chain or "swarm" of connectivity designed to illegally copy and share the exact same copyrighted file – could *not* constitute a "series of transactions or occurrences" for purposes of Rule 20(a).

Digital Sin, Inc. v. Does 1-176, 12-CV-00126 AJN, 2012 WL 263491 (S.D.N.Y. Jan. 30, 2012) (emphasis in original) (holding that 176 defendants were properly joined); *see also, OpenMind Solutions, Inc. v. Does 1-39*, C 11-3311 MEJ, 2011 WL 4715200 (N.D. Cal. Oct. 7, 2011) (holding the joinder of 39 defendants proper in a case with facts nearly identical to these), *and Hard Drive Productions, Inc. v. Does 1-55*, 11 C 2798, 2011 WL 4889094 (N.D. Ill. Oct. 12, 2011) (holding that joinder of 55 defendants at a similarly early stage of litigation was proper; but requiring plaintiff to amend its complaint for other reasons).

C. Contrary Cases

Courts are divided over whether joinder is proper in cases involving BitTorrent defendants. Many cases agree with the result recommended by this Magistrate Judge. *See, e.g., Digital Sin, Inc. v. Does 1-176*, 12-CV-00126 AJN, 2012 WL 263491 (S.D.N.Y. Jan. 30, 2012); *Donkeyball Movie, LLC., v. Does 1-171*, 810 F.Supp.2d 20 (D.D.C. 2011); *Hard Drive Productions, Inc. v. Does 1-55*, 11 C 2798, 2011 WL 4889094 (N.D. Ill. Oct. 12, 2011); *First Time Videos, LLC., v. Does 1-76*, 276 F.R.D. 254, 258 (N.D. Ill. 2011); *Nu Image, Inc. v. Does 1-3,932*, 2:11-CV-545-FTM-29, 2012 WL 646070 (M.D. Fl. Feb. 28, 2012). In several earlier cases, courts grappled with other peer-to-peer protocols[11] that are functionally distinct from the BitTorrent protocol. Additionally, several other courts have found joinder improper due to a lack of a concert of action. But, a concert of action is not required since Plaintiff alleges a right to relief severally against Defendants. Alleging a right to "several" relief is a proper route to joinder. Fed. R. Civ. P. 20(a)(2)(A).

[11] Such as Gnutella, Grokster, and Napster.

Cases reaching the opposite result are also factually or legally distinguishable. For example, the United States District Court for the District of Arizona recently held that joinder of 131 defendants was improper. *See Third Degree Films, Inc. v. Does 1-131*, 12-108-PHX-JAT, 2012 WL 692993 (D. Ariz. Mar. 1, 2012). In its discussion, the court said, "because pieces and copies of the protected work many [sic] be coming from various sources within the swarm, individual users might never use the same sources." *Third Degree Films*, 2012 WL 692993 *5. While this may be true, the reasoning avoids the relationship (traceable back to a specific initial seed through a series of transactions) that must exist between all users in the same Swarm. The *Third Degree Films* court also stated that, "[the swarm] can last for many months. During those months, the initial participants may never overlap with later participants." *Third Degree Films*, 2012 WL 692993 *5. However, the law of joinder does not have as a precondition that there be temporal distance or temporal overlap; it is enough that the alleged BitTorrent infringers participated in the same series of uploads and downloads in the same swarm.[12]

Several district courts in the Northern District of California have also considered cases against BitTorrent users, and have found joinder of large numbers of "Doe" defendants to be improper. In *Hard Drive Productions v. Does 1-188*, 809 F.Supp.2d 1150 (N.D. Cal. 2011), the court found that joinder of 188 BitTorrent users was improper. The court examined several older cases that addressed the issue of joinder with other methods of file transfer and appeared to be persuaded by similar arguments that there is a lack of concert of action by BitTorrent users and therefore joinder was not proper. *See Hard Drive Productions v. Does 1-188*, 809 F.Supp.2d at 1163. As discussed, concert of action, *i.e.*, a right to relief jointly, is not a precondition of joinder. Plaintiff asserts a right to relief jointly against Defendants *and* severally (Dkt. No. 1 at

[12] *See supra* discussion of *Mosley*, 497 F.2d 1333.

3). Therefore, the first clause of Rule 20(a)(2)(A) is satisfied by the assertion of a right severally.

The *Hard Drive Productions* court also reasoned that the various defenses may serve to demonstrate that joinder is improper. *See Hard Drive Productions*, 809 F.Supp.2d 1150 at 1164. However, "[t]he second prong of Rule 20(a) requires only that there be some common question of law or fact . . . not that all legal and factual issues be common to all [defendants]." *Disparte v. Corporate Executive Board*, 223 F.R.D. 7, 11 (D.D.C. 2004). The court in *Hard Drive Productions* decided that a plaintiff must show that the defendants were in the same swarm at the same time. *Hard Drive Productions*, 809 F.Supp.2d at 1164. This requirement, however, overlooks the thrust of the allegation that Defendants were part of the same swarm. That Defendants were all part of the same swarm demonstrates that they downloaded the Movie through a series of uploads and downloads from the same initial seeder. The *Hard Driver Productions* court also said,

> In this age of instant digital gratification, it is difficult to imagine, let alone believe, that an alleged infringer of the copyrighted work would patiently wait six weeks to collect the bits of the work necessary to watch the work as a whole. At the very least, there is no proof that bits from each of these addresses were ever assembled into a single swarm. As the court previously explained, under this court's precedent regarding other file sharing protocols, merely infringing the same copyrighted work over this period is not enough.

Hard Drive Productions, 809 F.Supp.2d at 1163.

But, it is not that an infringer would wait six weeks to receive the Movie, it is that the infringer receives the Movie in a few hours and then leaves his or her computer on with the Client Program uploading the Movie to other peers for six weeks. Because the Client Program's default setting (unless disabled) is to begin uploading a piece as soon as it is received and verified against the expected Hash, it is not difficult to believe that a Defendant who downloaded

the Movie on day one, would have uploaded the Movie to another Defendant or peer six weeks later. This consideration, however, is irrelevant since concerted action is not required for joinder.

Another contrary decision is found in *SBO Pictures, Inc. v. Does 1-3,036*, 11-4220 SC, 2011 WL 6002620 (N.D. Cal. Nov. 30, 2011). The *SBO Pictures* court determined that joinder of 3,036 defendants was improper, severed 3,035 defendants, and then maintained the action against defendant Doe 1. *Id.* The *SBO Pictures* opinion reads the term "closely" into Rule 20 and thus holds that Rule 20 requires "a series of closely related transactions." *Compare SBO Pictures, Inc. v. Does 1-3,036*, 11-4220 SC, 2011 WL 6002620 (N.D. Cal. Nov. 30, 2011), *with United Mine Workers of America v. Gibbs*, 383 U.S. 715, 724, 86 S.Ct. 1130, 1138, 16 L.Ed.2d 218 (1966); and *Pasha v. Jones*, 82 F.3d 418 (6th Cir. 1996) ("[claims may be joined if] they assert any right to relief relating to or arising out of the same transaction or . . . series of transactions . . . . Joinder is encouraged because it avoids multiple lawsuits involving similar or identical issues"), *and Disparte v. Corporate Executive Board*, 223 F.R.D. 7, 10 (D.D.C. 2004) ("[i]n order to satisfy [transactional relatedness] the claims must be logically related. . . . The logical relationship test is flexible"). There is no basis to conclude that an additional requirement of "closely related transactions" is contemplated by Rule 20, and to so conclude topples the plain reading of Rule's allowance of "a series of transactions."

Finally, in a case involving the same Plaintiff as this case, a recent Eastern District of Michigan decision found that joinder of 23 BitTorrent defendants was improper. *See Patrick Collins, Inc. v. John Does 1-23*, 11-CV-15231, 2012 WL 1019034 (E.D. Mich. Mar. 26, 2012). The court in that case found that -- for joinder purposes -- BitTorrent was indistinguishable from prior methods of internet file sharing, and then followed a line of cases holding that joinder was

improper in the context of those other methods of file sharing. This Magistrate Judge respectfully disagrees with that conclusion, and instead finds that the technology underlying BitTorrent does make it different from other file sharing methods, for joinder purposes. Joinder is proper in this case.

Since joinder is proper, the motion to sever must be denied. The motion to quash must also be denied; as a proper party, Doe 18 has no basis to quash the subpoena. Fed.R.Civ.P. 45(c)(3).

V. CONCLUSION

For the reasons set forth above, it is **RECOMMENDED** that Doe 18's motion to quash subpoena and dismiss this case be **DENIED**.

The parties to this action may object to and seek review of this Report and Recommendation, but are required to act within fourteen (14) days of service of a copy hereof as provided for in 28 U.S.C. § 636(b)(1) and Fed.R.Civ.P. 72(b)(2). Failure to file specific objections constitutes a waiver of any further right of appeal. *Thomas v. Arn*, 474 U.S. 140 (1985); *Howard v. Secretary of HHS*, 932 F.2d 505, 508 (6th Cir. 1991); *United States v. Walters*, 638 F.2d 947, 949-50 (6th Cir. 1981). The filing of objections which raise some issues, but fail to raise others with specificity, will not preserve all the objections a party might have to this Report and Recommendation. *Willis v. Secretary of HHS*, 931 F.2d 390, 401 (6th Cir. 1991); *Smith v. Detroit Fed'n of Teachers Local 231*, 829 F.2d 1370, 1373 (6th Cir. 1987). Pursuant to E.D. Mich. LR 72.1(d)(2), a copy of any objections is to be served upon this Magistrate Judge.

Within fourteen (14) days of service of any objecting party's timely filed objections, the opposing party may file a response. The response shall be no more than 20 pages in length

unless, by motion and order, the page limit is extended by the court. The response shall address each issue contained within the objections specifically and in the same order raised.

s/Mark A. Randon
Mark A. Randon
United States Magistrate Judge

Dated: April 5, 2012

Certificate of Service

I hereby certify that a copy of the foregoing document was served on the parties of record on this date, April 5, 2012, electronically.

s/Melody R. Miles
Case Manager to Magistrate Judge Mark A. Randon
(313) 234-5542

EXHIBIT C

Not Reported in F.Supp.2d, 2014 WL 656786 (N.D.Ill.)
(Cite as: 2014 WL 656786 (N.D.Ill.))

United States District Court, N.D. Illinois, Eastern Division.
TCYK, LLC, Plaintiff,
v.
Does 1–44, Defendants.

Case No. 13–cv–3825
1:13-cv-03825Filed February 20, 2014

Michael A. Hierl, Todd Sheldon Parkhurst, Hughes Socol Piers Resnick & Dym Ltd., Chicago, IL, for Plaintiff.

Alex Ogoke, Cardinal Legal Group, P.C., Kristen Elizabeth O'Neill, Levin Ginsburg, Chicago, IL, for Defendants.

MEMORANDUM OPINION AND ORDER

Robert M. Dow, Jr., United States District Judge

*1 Before the Court are four separate motions to sever defendants for improper joinder and/or quash third-party subpoenas, filed by two unspecified pro se John Does [18, 19], John Doe 11[21], and Defendant Babafemi George [24]. For the reasons stated below, the motions filed by the two John Does and Babafemi George [18, 19, and 24] are denied. John Doe 11's motion [21] is denied as moot, because Plaintiff has voluntarily dismissed John Doe 11 from the case without prejudice. See [30 and 41].

I. Background

On May 23, 2013, Plaintiff TCYK, LLC ("TCYK"), a motion picture producer and developer, brought this copyright infringement suit against forty-four John Does. TCYK alleges that each Defendant illegally downloaded and/or uploaded a copy of TCYK's motion picture "The Company You Keep," starring Robert Redford and Susan Sarandon, using computer software known as BitTorrent. BitTorrent is a software protocol that facilitates internet filesharing. Compared with the standard peer-to-peer file-sharing protocol in which one user downloads a file directly from another, BitTorrent allows users to download different small pieces of a file simultaneously from many users. Consequently, BitTorrent enables file-sharing at relative high speeds.

As Judge Tharp explained:

> To share information using BitTorrent, an initial file-provider (the "seeder") elects to share an initial file, called a "seed," with a torrent network. The file to be distributed is divided into segments called "pieces." Other users ("peers") intentionally connect to the seed file to download it. As each peer receives a new piece of the file, the peer also immediately becomes a source of that piece for other peers, relieving the original seeder from having to send that piece to every peer requesting a copy. This is the key difference between BitTorrent and earlier peer-to-peer file sharing systems: "BitTorrent makes file sharing a cooperative endeavor."

TCYK, LLC v. Does 1–87, 2013 WL 3465186, at *1 (N.D.Ill. July 10, 2013) (quoting *The Case Against Combating BitTorrent Piracy through Mass John Doe Copyright Infringement Lawsuits*, 111 Mich. L.Rev. 283, 290 (2012)).

Each user who downloads the seed file becomes a potential source of a piece of that file for peers who seek to download it subsequently. As more users download the file, thereby increasing the number of sources from which potential downloaders can take bits of that file, downloading speeds increase for future users. The users who download and upload the same seed file are called, collectively, a "swarm." Once a user who seeks to download a file connects to (effectively joining) an existing swarm, he continuously takes pieces of the seed file from the other users in the swarm until he has downloaded a completed file. Those sources

are, by definition, in the swarm because they have already downloaded the seed file. And that new swarm member who joined the swarm to download the file is now also a potential source of file bits for future downloaders who join the swarm. Swarm members are only a *potential* source, because users must be logged in to the BitTorrent software to share files. Therefore, swarm members must be logged in to the BitTorrent protocol simultaneously to be in the same swarm at the same time. See Compl. ¶ 4; see also *Malibu Media, LLC v. Reynolds*, 2013 WL 870618, at *2 (N.D.Ill. Mar. 7, 2013).

*2 TCYK alleges that John Does 1–44 participated in the same swarm to download and/or upload an identical version (*i.e.*, the same seed file) of The Company You Keep. Plaintiff does not know the true names of the Defendants at this time. Instead, Plaintiff knows the Internet Protocol ("IP") address assigned to each Defendant by his or her Internet Service Provider ("ISP"). Exhibit B to Plaintiff's complaint is a spreadsheet that, according to Plaintiff, captures the IP addresses, ISPs, and geographic locations of the forty-four John Doe Defendants, as well as the date and time that each IP address downloaded the common seed file. Plaintiff believes that discovery will lead to the true names of the Defendants, at which time Plaintiff intends to amend its complaint with that information.

To that end, Plaintiff has issued third-party subpoenas to the ISPs identified on Exhibit B, seeking the identities and personal information associated with the corresponding IP addresses. Several Defendants, having been informed of the subpoena (and this lawsuit) by their ISP, now seek to quash the subpoena and/or sever all defendants for improper joinder. More specifically:

- An unspecified John Doe argues [18] that Plaintiff has improperly joined the forty-four Defendants because Plaintiff does not allege that they participated in the same swarm *at the same time*, such that Federal Rule of Civil Procedure 20(a)(2) requires the Court to dismiss forty-three of them from the case.

- Another unspecified John Doe makes the same argument [19] and, in the alternative, argues that Plaintiff's third-party subpoena to his ISP provider should be quashed because the person to whom the IP address is assigned may not be the only person who accessed the internet through that address.

- Babafemi George, who purports to be a Defendant but does not identify himself by John Doe number or IP address, seeks [24] to quash Plaintiff's subpoena, because—seemingly confused as to whom the subpoena is directed—he is not in possession of the requested documents and has no knowledge of the alleged infringement.

II. Analysis

A. Motion to Sever for Improper Joinder

Rule 20 of the Federal Rules of Civil Procedure governs permissive joinder of defendants. It states: "Persons ... may be joined as defendants if: (A) any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and (B) any question of law or fact common to all defendants will arise in the action." Fed. R. Civ. P. 20(a)(2). John Doe Defendants argue that Plaintiff has failed to allege that the forty-four Defendants in this case engaged in either the same transaction or the same series of transactions. Although Plaintiff alleges that Defendants participated in the same swarm (*i.e.*, that they downloaded, and therefore may also have distributed, the same seed file), Plaintiff acknowledges that Defendants may not have participated in the swarm *at the same time*. See Compl. ¶ 4 (noting that a swarm member is only a source of the file for future downloaders if the swarm member is online at the time that the subsequent peer downloads the file). Plaintiff

argues, however, that Defendants' actions comprise the same series of transactions or occurrences for the purpose of Rule 20, by virtue of the cooperative and interdependent nature of the BitTorrent platform.

Exhibit B to TCYK's complaint sets out the exact dates and times at which the forty-four Defendants allegedly downloaded the movie. The forty-four downloads took place over the span of thirty days, from April 14, 2013 to May 14, 2013. Defendants argue that this underscores the unrelatedness of their actions and the improbability that all forty-four participated in the swarm simultaneously. Defendants argue that, absent an allegation that these forty-four users shared file bits with each other, they cannot be considered to have participated in the same transaction. And absent an allegation that they were necessary links in the file's chain of custody, they cannot be considered to have participated in the same *series* of transactions. Defendants contend that their only connection to each other is that they each allegedly downloaded the same seed file, and that they therefore did not engage in the "same transaction, occurrence, or series of transactions or occurrences" within the meaning Rule 20. Implicit in their argument is that—given the likelihood that this swarm consisted of far more than the forty-four Defendants named in this suit (sued here only because of their physical location in this district)—there is a possibility that not one user among the forty-four Defendants shared a single file bit with another user in this group.

*3 There is a split of authority in this district over the appropriateness of joining defendants who are alleged to have participated in the same BitTorrent swarm. *Compare, e.g., Reynolds,* 2013 WL 870618 at * 2 (finding joinder improper because "[w]here a swarm continues to exist for an extended period of time, it is improbable that defendants entering a swarm weeks or months apart will actually exchange pieces of data."), *with reFX Audio Software, Inc. v. Does 1–111,* 2013 WL 3867656, at *3 (N.D.Ill. July 23, 2013) ("[T]he argument that joinder is appropriate only if defendants participated in the same swarm at the same time ... ignores the fact that permissive joinder under Rule 20(a) does not require that defendants act in concert with each other, nor does it have as a precondition that there be a temporal distance or temporal overlap.") (internal citations and quotations omitted). The debate centers on whether participation in a swarm constitutes the requisite "series of transactions or occurrences" contemplated by Rule 20, in light of the interdependent quality about BitTorrent file sharing. Rule 20 does not define "series of transactions or occurrences," but there is momentum building in this district in favor of the Federal Circuit's recent articulation of the phrase's meaning. See *Zambezia Film PTY, LTD. v. Does 1–65,* 2013 WL 4600385, at *4 (N.D.Ill. Aug. 29, 2013); *reFX Audio Software,* 2013 WL 3867656 at *3; *Malibu Media, LLC v. John Does 1–6,* 291 F.R.D. 191, 199–200 (N.D.Ill. May 17, 2013). To date, the Federal Circuit is the only federal court of appeals that has addressed the issue. Tracing the rule's history, past application, and interpretation of the phrase "transaction or occurrence" in other contexts, the Federal Circuit noted that "the mere fact that a case involves independent actors as defendants does not necessarily bring the case outside the scope of Rule 20." See *Malibu Media,* 291 F.R.D. at 200 (quoting *In re EMC Corp.,* 677 F.3d 1351, 1358 (Fed. Cir. 2012)). Citing both the Wright and Miller treatise and Supreme Court case law, the Federal Circuit concluded that "independent defendants satisfy the transaction-or-occurrence test of Rule 20 when there is a logical relationship between the separate causes of action." *Id.* at 1356. "The flexibility of this standard enables federal courts to promote judicial economy by permitting all reasonably related claims for relief by or against different parties to be tried in a single proceeding under the provisions of Rule 20." *Malibu Media,* 291 F.R.D. at 201 (quoting Charles Alan Wright, *et al., Federal Practice and Procedure* § 1652 (3d ed.1998).

The Court acknowledges the strong arguments on both sides of the issue, but agrees with the weight of the authority and growing trend in this district that participation in a swarm qualifies as engaging in a "series of transactions or occurrences" for the purpose of Rule 20. As other judges in this district have concluded, a user who connects to a swarm joins a "cooperative endeavor." *TCYK, LLC*, 2013 WL 3465186 at *1. Regardless of whether these forty-four defendants contemporaneously participated in the swarm, shared bits of the seed file with each other, or even shared bits of the file at all, each joined the swarm knowing that his participation increased the swarm's ability to disseminate a common seed file quickly and efficiently. The Court therefore concludes that a logical relationship exists among the actions of the Defendants such that joinder is proper. Moreover, joinder here serves the interest of judicial economy, which underlies Rule 20. Wright *et al., supra*, § 1653. "At the pleading stage, it is more efficient to join Doe Defendants in one action than to require separate lawsuits. Individual litigations, at least at the early stages of litigation, would be needlessly expensive for both [Plaintiff] and the courts and would frustrate the judicial efficiency policies at the heart of Rule 20." *Malibu Media*, 291 F.R.D. at 204–05. Accordingly, at this stage of the ligation, the Court denies Defendants' motions to sever for improper joinder.

B. Motion to Quash Subpoena

Although none of the Defendants cite to a specific rule or rely on any authority as the basis for their motions challenging the validity of Plaintiff's subpoenas to Defendants' ISPs, motions to quash are governed by Rule 45 of the Federal Rules of Civil Procedure. Rule 45 provides that a court must quash or modify a subpoena that (1) fails to allow a reasonable time to comply; (2) requires a person who is neither a party nor a party's officer to travel more than 100 miles; (3) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or (4) subjects a person to undue burden. Fed. R. Civ. P. 45(c)(3)(A)(i)-(iv). The party seeking to quash the subpoena bears the burden of demonstrating that it falls within one of the Rule 45 categories. *reFX Audio Software*, 2013 WL 3867656 at *3; *Pacific Century Int'l, Ltd. v. Does 1–37*, 282 F.R.D. 189, 193 (N.D.Ill.2012). Ruling on motions to quash lies within the sound discretion of the district court. See *Griffin v. Foley*, 542 F.3d 209, 223 (7th Cir. 2008).

*4 One of the unspecified John Doe Defendants argues that the subpoenas should be quashed, because the person to whom an IP address is assigned may not be the person who actually downloaded TCYK's movie. According to Defendant, an IP address is often associated with a wireless router, not a specific computer. And the name associated with a particular IP address is that of the person who pays the internet bill. Consequently, various people (family members, roommates, opportunistic neighbors, patrons at an internet café) may be using the internet under a single IP address at any given time. Defendant argues that the subpoenas should be quashed on account of the uncertainty this creates and the potential unfairness to an innocent IP addressee.

Construing this pro se Defendant's motion liberally, he seems to argue that the subpoenas impose an undue burden under Rule 45. To the extent that Defendant attempt to advance this argument, he first needs standing to do so. "A party has standing to move to quash a subpoena addressed to another if the subpoena infringes upon the movant's legitimate interests." *Zambezia Film PTY*, 2013 WL 4600385 at *2 (quoting *United States v. Raineri*, 670 F.2d 702, 712 (7th Cir. 1982)). Here, we need not decide whether Defendant has standing to challenge the subpoena, because he has not demonstrated that the subpoena imposes an undue burden on him. The Court agrees with the position consistently taken by the other Judges in this district—namely, that a subpoena directed at an ISP does not impose an undue burden on a defendant, because it does not require him to do anything. See *reFX Audio Software*, 2013 WL

3867656 at *3; *Reynolds*, 2013 WL 870618 at * 2; *Sunlust Pictures, LLC v. Does 1–75*, 2012 WL 3717768, at *2 (N.D.Ill. Aug. 27, 2012).

To the extent that Defendant is arguing that the information the subpoenas seek is not relevant, and thus prohibited by Rule 26(b)(1), the Court also denies the motion to quash. "Parties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody, condition and location of any documents or tangible things and the identity and location of persons who know of any discoverable matter." Fed. R. Civ. P. 26(b)(1). Relevant information need not be admissible at trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. *Id.* Here, the information sought by the subpoenas is highly relevant to TCYK's claims. Even if the person associated with the IP address is not the person who allegedly downloaded The Company You Keep, obtaining the IP addressee's information is the logical first step in identifying the correct party. Moreover, without the subpoenas TCYK would have no way of prosecuting its copyright infringement claims. For these same reasons, the Court found good cause to grant Plaintiff's request to serve these third-party subpoenas prior to a Rule 26(f) conference. See Court Order Granting Pl. Mot. for Leave to Take Discovery, June 27, 2013[12]. Accordingly, and consistent with the approach taken by the other judges in this district, the Court denies Defendant's motion to quash, to the extent it argues that the information sought is irrelevant. See *e.g.*, *Zambezia Film PTY*, 2013 WL 4600385 at *2; *reFX Audio Software*, 2013 WL 3867656 at *2; *Malibu Media*, 291 F.R.D. at 197.

Finally, the Court denies Defendants' motions to quash to the extent that Defendants contend that they are not the persons who downloaded The Company You Keep at the respective IP address associated with their name. See *e.g.*, Def. Babafemi George Mot. to Quash [24] (noting that he is "unable to provide the plaintiff with the requested documents because the defendant was not at home during the time and date in question and had no knowledge of the alleged infringement"). That is a general denial of liability, which is not an appropriate basis for quashing a subpoena. See *Purzel Video GmbH v. Does 1–108*, 2013 WL 6797364, at *4 (Dec. 19, 2013); *Malibu Media*, 291 F.R.D. at 197; *First Time Videos, LLC v. Does 1–76*, 276 F.R.D. 254, 256 (N.D.Ill.2011) (collecting cases). Accordingly, Defendants' motions to quash are denied.

III. Conclusion

*5 For the reasons stated above, Defendants' motions to sever for improper joinder and/or quash third-party subpoenas, filed by two unspecified pro se John Does and Defendant Babafemi George [18, 19, and 24] are denied. John Doe 11's motion [21] is denied as moot, because Plaintiff has voluntarily dismissed John Doe 11 from the case without prejudice. See [30 and 41].

N.D.Ill., 2014
TCYK, LLC v. Does 1-44
Not Reported in F.Supp.2d, 2014 WL 656786 (N.D.Ill.)

END OF DOCUMENT