IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Headhunter, LLC, *Plaintiff,* v. Does 1–17, *Defendants*.	§ § § § § § § § § § § § §	Case No. 4:17-cv-2352 Jury

PLAINTIFF HEADHUNTER, LLC'S *EX PARTE* MOTION TO TAKE PRE-26(F) CONFERENCE DISCOVERY OF THIRD-PARTY INTERNET SERVICE PROVIDER

COURT PROCEDURE NOTE

Due to the ex parte *nature of this motion and the fact that there will be no opposition as all Doe defendants cannot be identified if and until the Court rules favorably, the Court may wish to consider this motion prior to the typical submission date.*

TABLE OF CONTENTS

Page

I. MOTION 1

II. INTRODUCTION 2

III. NATURE AND STAGE OF THE PROCEEDING 5

IV. ISSUE TO BE RULED UPON AND STANDARD OF REVIEW 6

V. A SHORT SUMMARY OF THE ARGUMENT 7

VI. ARGUMENT 9

A. Plaintiff Has Made a Concrete Showing of a Prima Facie Claim of Actionable Harm 9

B. Plaintiff Has Proposed Clear and Specific Discovery 10

C. Plaintiff Has No Alternative Means to Obtain the Information 12

D. Plaintiff Needs the Subpoenaed Information to Advance the Claim 13

E. Plaintiff's Interest in Obtaining the Subscribers' True Identities Outweighs Subscribers' Interest in Remaining Anonymous 14

VII. CONCLUSION 16

TABLE OF EXHIBITS

Tab

Fischman Declaration 1

NOTE: Plaintiff has provided internet links for all background reading referenced in this motion to avoid submitting voluminous exhibits. Plaintiff will submit copies of any background material referenced in this motion upon request.

TABLE OF UNREPORTED CASES

App. Page

Garrett v. Comcast Comms., Inc.,
No. 3:04-cv-693 (N.D. Tex. July 23. 2004) 1

W. Coast Prods., Inc. v. Does 1-351,
No. 4:12-cv-00504, 2012 WL 2577551 (S.D. Tex. July 3, 2012)..... 3

Well Go USA, Inc. v. Unknown Participants,
No. 12-cv-00963, 2012 WL 4387420 (S.D. Tex. Sept. 25, 2012) 7

TABLE OF AUTHORITIES

CASES

Arista Records, LLC v. Doe 3,
604 F.3d 110 (2d Cir. 2010) 7

Bell Atl. Corp. v. Twombly,
127 S. Ct. 1955 (2007).....9

Columbia Ins. Co. v. Seescandy.Com,
185 F.R.D. 573 (N.D. Cal. 1999) 10

Garrett v. Comcast Comms., Inc.,
No. 3:04-cv-693 (N.D. Tex. July 23, 2004) 12

General Universal Sys., Inc. v. Lee,
379 F. 3d 131 (5th Cir. 2004) 9

In re Verizon Internet Servs., Inc.,
257 F. Supp. 2d 244 (D.D.C. 2003).....14

Patrick Collins, Inc. v. John Doe 1,
945 F. Supp. 2d 367 (E.D.N.Y. 2013).....9

Qwest Comms. Int'l, Inc. v. Worldquest Networks, Inc.,
213 F.R.D. 418 (D. Colo. 2003) 13

Recording Indus. v. Verizon Internet,
351 F. 3d 1229 (D.D.C. 2003).....12

Sony Music Entm't Inc. v. Does 1–40,
326 F. Supp. 2d 556 (S.D.N.Y. 2004) 10, 15

St. Louis Grp., Inc. v. Metals & Additives Corp., Inc.,
275 F.R.D. 236 (S.D. Tex. 2011) 6

W. Coast Prods., Inc. v. Does 1-351,
No. 4:12-cv-504, 2012 WL 2577551 (S.D. Tex. July 3, 2012)..... 5, 11, 15

Well Go USA, Inc. v. Unknown Participants,
No. 12-cv-963, 2012 WL 4387420 (S.D. Tex. Sept. 25, 2012) 7

STATUTES

17 U.S.C. § 512(h) 12

47 U.S.C. § 551(1)(a)..... 8, 15

47 U.S.C. § 551(c)(1)(B) 13

47 U.S.C. § 551(c)(2).....13
47 U.S.C. § 551(e) 13

RULES

FED. R. CIV. P. 26(d)(1).....6, 7
FED. R. CIV. P. 26(f) 6
FED. R. CIV. P. 45 1

I. MOTION

Plaintiff, Headhunter, LLC ("Headhunter"), hereby moves this Court *ex parte* requesting an order granting limited pre-Rule 26(f) conference discovery. Specifically, plaintiff seeks to issue a subpoena to an internet service provider ("ISP") AT&T pursuant to FED. R. CIV. P. 45 for information sufficient to identify each defendant (currently listed as Does 1–17), including name, current and permanent address, telephone number, and e-mail address.

Each Doe defendant has been observed as using torrent networks to distribute an infringing copy of plaintiff's copyrighted motion picture. However, plaintiff has only been able to identify each defendant by the internet protocol ("IP") address the defendant used to commit the infringement. *See* Exhibit 2 to the Complaint. It is therefore necessary for plaintiff to obtain the identity of the subscriber corresponding to the IP address to investigate the Defendant's identities.

ISPs routinely provide the identity of a subscriber corresponding to an IP address under the Digital Millennium Copyright Act ("DMCA"), and in fact, the ISPs often provide a special facsimile number for facilitating service of this type of subpoena when issued by law enforcement officials.

Plaintiff will use any obtained information solely for protecting Plaintiff's rights as set forth in its Complaint.

II. INTRODUCTION

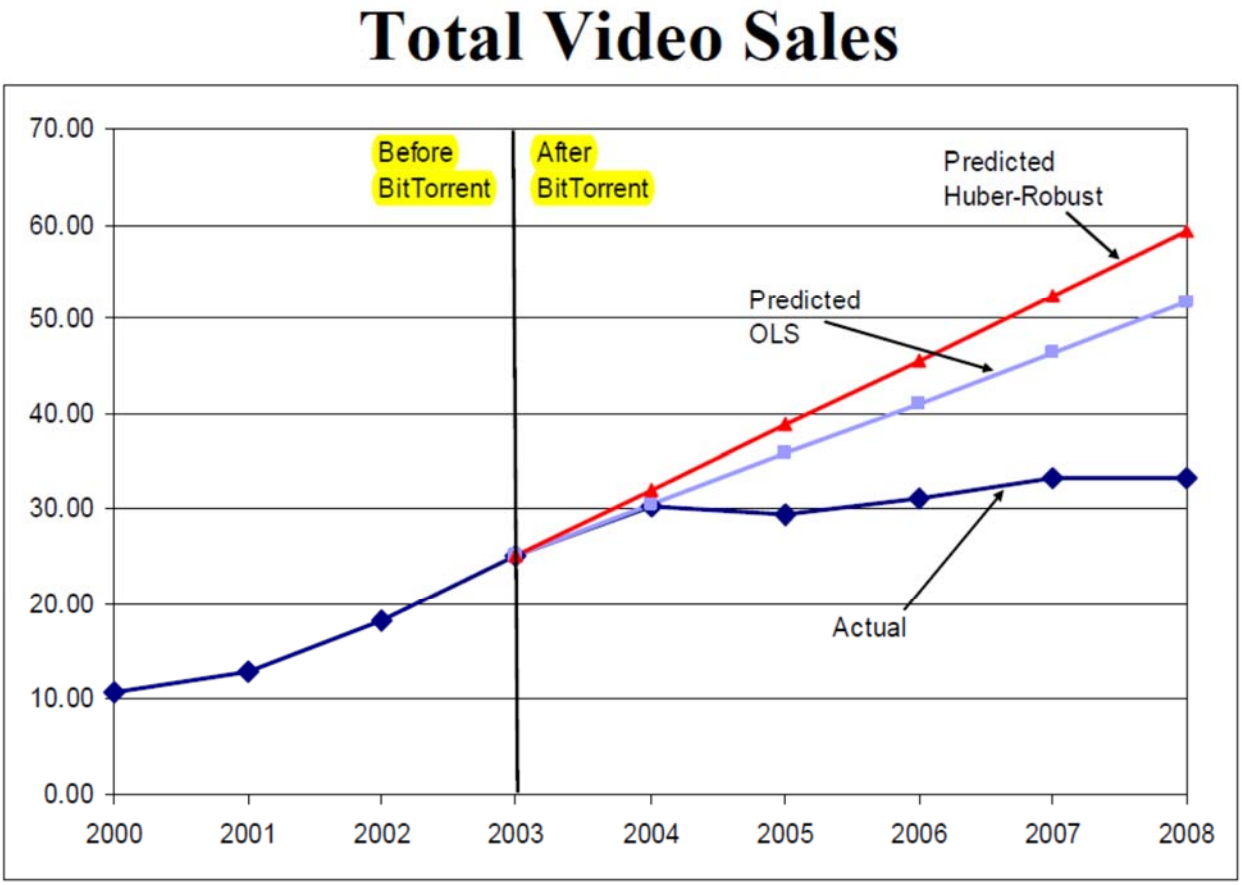
A 2015 U.S. Executive Report noted that unauthorized distribution of motion picture recordings via the Internet is doing tremendous damage to film producers, distributers, and copyright holders.[1] This economic harm is illustrated in the graphs below from a University of Texas research paper, showing the precipitous decline in video and DVD sales coinciding with the rise of BitTorrent file sharing.[2]

---

[1] Ambassador Froman, 2015 Special 301 Report, Executive Office of the President of the United States (finding unauthorized recordings of first-run motion pictures result in economic harm not only in the market where the film was originally shown, but in other markets as well and that governments must not create "a domestic environment that offers a safe haven for piracy on the Internet"), *available at* https://ustr.gov/sites/default/files/2015-Special-301-Report-FINAL.pdf.

NOTE: Plaintiff has provided internet links for all background reading referenced in this motion to avoid submitting voluminous exhibits. Plaintiff will submit copies of any background material referenced in this motion upon request.

[2] Zentner, *Measuring the Impact of File Sharing on the Movie Industry: An Empirical Analysis Using a Panel of Countries*, at 2 & 23, University of Texas at Dallas (Mar. 22, 2010), *available at* http://ssrn.com/abstract=1792615 ("Our findings, in short, indicate that the unauthorized downloading of movies decreases video sales by a substantial amount.").



The Department of Justice is addressing this plague of BitTorrent infringement. In July 2016, the DOJ announced the arrest of the mastermind behind the most visited illegal file-sharing website, *Kickass Torrents*.[3] A criminal complaint filed in Chicago charges him with conspiracy to commit money laundering and criminal copyright infringement. The DOJ estimates this one website was responsible for

[3] *U.S. Authorities Charge Owner of Most-Visited Illegal File-Sharing Website with Copyright Infringement*, Dept. of Justice Press Release (July 20, 2016), *available at* https://www.justice.gov/opa/pr/us-authorities-charge-owner-most-visited-illegal-file-sharing-website-copyright-infringement.

unlawfully distributing well over $1 billion of copyrighted materials and was the 69th most frequently visited website on the internet.

And Texas Representative Lamar Smith further notes with respect to such BitTorrent internet havens like these that:

> The growing number of foreign websites that offer counterfeit or stolen goods continues to threaten American technology, products and jobs. Illegal counterfeiting and piracy costs the U.S. economy $100 billion and thousands of jobs every year.[4]

Unfortunately, while the DOJ has charged by criminal complaint the owner of one site, there are countless other similar websites, operating from remote corners of the world that continue to facilitate illegal distribution of motion pictures, music and ebooks, using BitTorrent software. Downloaders can even consult "top ten pirated movie lists" to steer them to the hottest titles.

Locally, the University of Houston announced it will block BitTorrent peer-to-peer data traffic on the University of Houston Wi-Fi network "to limit illegal downloading of copyrighted material and comply with state

[4] Smith, Lamar: Why We Need a Law Against Online Piracy (Jan. 1, 2012), *available at* www.cnn.com/2012/01/20/opinion/smith-sopa-support/index.html.

and federal laws."[5]

Headhunter is a victim of such piracy. Plaintiff owns the copyright for the movie A Family Man ("Motion Picture"), a mainstream motion picture with well-known actors. [Dkt. 1 ¶¶ 30–31 & Ex. 1.] Although the movie was released in the U.S. only recently, already Headhunter has identified 17 IP addresses located in the Southern District of Texas as participating in a group copying and distribution of an unauthorized copy of Headhunter's Motion Picture, without license, via an online peer-to-peer ("P2P") torrent network system. [Dkt. 1 ¶¶ 45–51 & Ex. 2.]

III. NATURE AND STAGE OF THE PROCEEDING

In an attempt to stop this unauthorized distribution of the Motion Picture, plaintiff filed a Complaint alleging copyright infringement. [Dkt. 1.] For each defendant, Plaintiff was only able to identify the defendant infringer by the IP address the infringer used to commit the infringement. [*Id*.] As explained in the Complaint, only the ISP knows which subscribers were associated with the IP addresses at the relevant times. As such, Plaintiff named pseudonymous "Doe" defendants associated with the IP addresses, as is convention. *See, e.g.*, *W. Coast Prods., Inc. v. Does 1–351*, No. 4:12-cv-504, 2012 WL 2577551 (S.D. Tex. July 3, 2012) (Doc. 30)

[5] University of Houston IT Notice, *available at* http://rationalrights.com/?p=502.

(Atlas, J.) (App., Tab B at App. 3).

Now, Plaintiff is filing this *ex parte* motion to serve a subpoena on the ISP so that plaintiff may obtain the identities of the account holders corresponding to the IP addresses at the times plaintiff observed the infringement. Having the ability to issue a subpoena on the relevant ISP will allow plaintiff to contact the subscriber and, if necessary, amend the Complaint and serve the same.

IV. ISSUE TO BE RULED UPON AND STANDARD OF REVIEW

Plaintiff seeks an order permitting limited, pre-Rule 26(f), discovery from a third-party for the sole purpose of identifying the Doe defendants. FED. R. CIV. P. 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)" unless the Court orders otherwise, and this Court has adopted a "good cause" standard to determine whether to permit such expedited discovery. *St. Louis Grp., Inc. v. Metals & Additives Corp., Inc.*, 275 F.R.D. 236, 240 (S.D. Tex. 2011).

When considering if "good cause" exists for motions to identify the accounts associated with IP addresses, this Court considers: "(1) a concrete showing of a prima facie claim of actionable harm by the plaintiff; (2) specificity of the discovery request; (3) the absence of alternative means to

obtain the subpoenaed information; (4) a central need for the subpoenaed information to advance the claim; and (5) the user's expectation of privacy." *Well Go USA, Inc. v. Unknown Participants*, No. 4:12-cv-963 (S.D. Tex. Sept. 25, 2012) (Ellison, J.) (App., Tab C at App. 8–9) (citing *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 114 (2d Cir. 2010)).

V. A SHORT SUMMARY OF THE ARGUMENT

Plaintiff has set forth in detail a *prima facie* case that its copyright has been, and is being, infringed by people whom plaintiff can now only identify by the IP addresses they used in committing the infringement. Plaintiff has filed suit and wishes to use discovery requested in this motion to identify the true identities of these infringers. But the default Federal Rules—written for the typical case where the true identity of the defendant is known to plaintiff—specify that discovery can only be initiated after the plaintiff and defendant's conference. *See* 26(d)(1). Yet, to confer, plaintiff needs the sought-after discovery to know with whom to confer.

To break this "Catch 22," Headhunter proposes obtaining specific, limited, information regarding the identity of the subscribers who were responsible for these IP addresses at the times of observed infringement from their ISP—the only entity that can identify those persons. To minimize any burden on the ISP, plaintiff is requesting minimal

information it needs to advance the litigation—information ISPs regularly provide to copyright owners in the DMCA context. Because the ISPs only keep the needed data for a limited time, without the relief sought, plaintiff's opportunity to identify the defendants may soon be lost forever.

Finally, while defendants may be hoping to maintain the anonymity the Internet affords to infringe with impunity, Does 1–17 should not expect it. Semi-anonymous peoples from around the world have been using BitTorrent technology to illegally copy the Motion Picture from computers connected to the BitTorrent community through the subscriber's internet account. The subscriber should not be heard to complain when the owner of the copyright asks the subscriber's ISP to provide information to identify the subscriber. Indeed, by statute, ISPs initially and regularly notify subscribers that their information is subject to disclosure via court order. 47 U.S.C. § 551(1)(a)1. And defendants' willful violation of copyright law is just the type of activity that would invite such a court order.

In short, for plaintiff to advance its claim and seek relief from the harm done by defendants—people who should have no expectation of privacy for their illegal activity—the Court should allow the narrowly tailored discovery to the sole source of the information, the ISP.

VI. ARGUMENT

The following subsections establish why the good cause factors all favor allowing plaintiff's requested, early, third-party discovery.

A. Plaintiff Has Made a Concrete Showing of a Prima Facie Claim of Actionable Harm

"To establish a prima facie case of copyright infringement, a copyright owner must prove (1) ownership of a valid copyright and (2) copying by the defendant of constituent elements of the work that are original." *General Universal Sys., Inc. v. Lee*, 379 F. 3d 131, 141 (5th Cir. 2004) (internal quotes, citations, and modifications removed). At the pleading stage, a plaintiff simply must provide "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 127 S. Ct. 1955, 1974 (2007). And "plausible" simply means having an appearance of truth or reason, a lower threshold than a "reasonable likelihood" standard. *See Patrick Collins, Inc. v. John Doe 1*, 945 F. Supp. 2d 367, 376 (E.D.N.Y. 2013).

As to the first element, copyright interest, plaintiff filed a copyright certificate for A Family Man, [Dkt. 1 Ex. 1], which "is prima facie evidence both that a copyright is valid and that the registrant owns the copyright." *General Universal Sys.*, 379 F. 3d at 141.

As to the second element, evidence of copying, Maverickeye UG

("Maverickeye"), a company that specializes in internet monitoring illegal P2P distribution of material, such as motion pictures, has detected and logged IP addresses that have distributed an unauthorized copy of plaintiff's Motion Picture. These IP addresses, along with the dates and times during which the distribution took place, are listed in the exhibit attached to the complaint. [Dkt. 1 Ex. 2; Ex. 1, Fischman Decl. ¶3.]

Further, through geolocation services, including the Maverickeye software's geolocation feature, it was confirmed that at the time of these activities, these IP addresses were located in the Southern District of Texas. [Ex. 1, Fischman Decl. ¶4.]

B. Plaintiff Has Proposed Clear and Specific Discovery

The relevant inquiry is whether "[p]laintiffs' discovery request is . . . sufficiently specific to establish a reasonable likelihood that the discovery request would lead to identifying information that would make possible service upon particular defendants who could be sued in federal court." *See Sony Music Entm't Inc., v. Does 1-40*, 326 F. Supp. 2d. 556, 566 (S.D.N.Y. 2004) (citing *Columbia Ins. Co. v. Seescandy.Com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999)).

Here, plaintiff's discovery request satisfies this requirement by asking for the subscriber information that corresponds to an IP address at a specific date and time where infringing activity was observed. It is

reasonable to suspect that this subscriber conducted the alleged activity, but even if the IP addresses cannot pinpoint a person responsible for a particular file download this Court has found that:

> Nevertheless, it is reasonable to use an IP address as a starting point to obtain identifying information about a Doe Defendant who, through digital forensic means, has been tied to the torrent swarm in issue. The identifying information allows Plaintiff to make a good faith investigation into whether a particular individual has a reliable factual connection to the IP address associated with the swarm.

W. Coast Prods., No. 4:12-cv-504 (App., Tab B at App. 5). At a minimum, obtaining the subscriber information will allow plaintiff's counsel to assess whether pursuit of claims is in fact feasible once the individual associated with the IP address has been identified.[6] As discussed in the following subsection, plaintiff has no other way to do this.

The subpoena is narrowly tailored to get the required information, and as this is the type of data normally kept in the regular course of business, the request should impose minimal burden on the ISP. Indeed, for almost 20 years, in other situations, Congress has provided copyright holders the

[6] The situation is analogous to capturing the license plate of a car that committed a violation. The driver is likely the owner, but, if not, the owner is the person most liable to know who was driving his or her car at the time of the incident.

ability to serve subpoenas for this type of information regarding works stored on an ISP server without having to file a lawsuit or motion a court. *See* DMCA, Pub. L. No. 105–304, 112 Stat. 2860 (Oct. 28, 1998) (codified at 17 U.S.C. § 512(h)).[7] As such, ISPs are already well equipped to handle these routine requests.

C. Plaintiff Has No Alternative Means to Obtain the Information

Although Headhunter's agents are able to observe defendants' infringing activity through forensic software, plaintiff is unable to access defendants' identifying information, other than the IP addresses they used to commit the infringement. [Ex. 1, Fischman Decl. ¶6.] Plaintiff is likewise unable to upload a file onto defendants' computers or otherwise communicate with defendants in a manner that would provide notice of suit. Hence, plaintiff must contact the ISP the defendants used when committing the infringement to learn the subscriber's information to communicate with them and/or amend the Complaint to use defendants' true names.

---

[7] However, this provision does not appear to contemplate the situation where an ISP is acting as a conduit for P2P file sharing, which is understandable because at the time of the DCMA, P2P software like BitTorrent was "not even a glimmer in anyone's eye." *Recording Indus. v. Verizon Internet*, 351 F. 3d 1229, 1238 (D.D.C. 2003) (citation omitted). It appears this issue has not been decided in this district or circuit. *See, e.g.*, *Garrett v. Comcast Comms., Inc.*, No. 3:04-cv-693, n.1 (N.D. Tex. July 23, 2004) [Dkt. 15] ("This Court is not bound to follow the precedent of *RIAA v. Verizon*."). (App., Tab A at App. 2).

But plaintiff cannot simply ask the ISP for the requested information. Under the Cable Communications Policy Act of 1984, as amended:

> [A] cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.

47 U.S.C. § 551(c)(1)(B). As such, the ISP requires a subpoena to release the name and address of subscribers. *Id.* § 551(c)(2).

Moreover, time is of the essence. Per statute, "[a] cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information." *Id.* § 551(e). Therefore, if the subpoenas are not issued quickly, the subscriber information may be permanently lost. *See Qwest Commc'ns Int'l, Inc. v. Worldquest Networks, Inc.*, 213 F.R.D. 418, 419 (D. Colo. 2003) (recognizing expedited discovery may be appropriate if "physical evidence may be consumed or destroyed with the passage of time").

D. Plaintiff Needs the Subpoenaed Information to Advance the Claim

The information that plaintiff seeks to subpoena from the ISPs is

necessary to advance its claims against the infringers. Because the ISPs are not named defendants, this is not a case of whether to provide immediate access to the requested discovery rather than postponing its ultimate production until the normal course of discovery. Rather, the information requested is a prerequisite needed so that: (1) the defendants may be notified so that they may answer; (2) the Court may have a complete and informed Case Management Conference with defendants present; and (3) litigation, including normal discovery, can commence. The subscriber information simply must be identified before this suit can progress further.

E. Plaintiff's Interest in Obtaining the Subscribers' True Identities Outweighs Subscribers' Interest in Remaining Anonymous

Plaintiff has a strong and legitimate interest in protecting its copyrighted content, and has established it cannot advance its claims without the ability to identify the individuals responsible for downloading and distributing plaintiff's copyrighted movie. In contrast, the subscribers cannot make a sound claim to retaining their anonymity.

First, the subscribers have little expectation of privacy because they voluntarily allowed their internet accounts to be used to distribute copyrighted information to others through P2P file sharing. *In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 267 (D.D.C. 2003), *rev'd on other grounds*, *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet*

Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) ("[I]f an individual subscriber opens his computer to permit others, through peer-to-peer file-sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world.").

Second, the subscribers are on notice that AT&T prohibits its internet service for any use that infringes any material that is protected by copyright law[8] and that their personal information may be disclosed to "[c]omply with court orders, subpoenas, lawful discovery requests …." [9]

Indeed, the Cable Act requires ISPs to notify customers of the possibility of this disclosure at the time of entering into an agreement to provide service and at least once a year thereafter. § 551(1)(a).

Third, "to the extent that anonymity is used to mask copyright infringement or to facilitate such infringement by others, the First Amendment is no protection." *W. Coast Prods.*, No. 4:12-cv-504 (App., Tab B at App. 5) (citing *Sony Music Entm't Inc. v. Does 1–40*, 326 F. Supp.

---

[8] AT&T Internet Terms of Service / att.net Terms of Use for Internet Service(s) at section 10.b., *available at https://www.att.com/legal/terms.internetAttTermsOfService.html#.*

[9] AT&T's Full Privacy Policy at Question No. 4 About Information Sharing, *available at* http://about.att.com/sites/privacy_policy/full_privacy_policy.

2d 556, 567 (S.D.N.Y. 2004) ("[D]efendants' First Amendment right to remain anonymous must give way to plaintiffs' right to use the judicial process to pursue what appear to be meritorious copyright infringement claims.")).

Fourth, it is standard procedure for ISPs to provide subscribers with sufficient time to make an appearance to object to the disclosure of the subscriber's information, request a protective order, or request other relief. Therefore, if the subscribers wish to argue that their information should not be publicly disclosed, they will have an opportunity to be heard.

VII. CONCLUSION

As shown above, every factor the Court considers when determining if good cause exists militates in favor of allowing the pre-26(f) conference discovery. Therefore, Headhunter respectfully requests the Court to grant its motion. A proposed Order is attached.

Dated: August 3, 2017

Respectfully submitted,
s/Gary J. Fischman/

Gary J. Fischman, attorney-in-charge
Tex. State Bar No. 787469
S.D. Tex. Bar No. 17126
FISCHMAN LAW PLLC
710 N. Post Oak Rd. Suite 105
Houston, TX 77024–3808
Tel: 713.900.4924
fischman@fischmaniplaw.com

Attorney for Plaintiff,
Headhunter, LLC

CERTIFICATE OF SERVICE PER LR5

As the true identities of the defendants are unknown at this time, service is not possible and this motion is being filed *ex parte*.

Dated: August 3, 2017 s/Gary J. Fischman/
Gary J. Fischman

CERTIFICATE OF CONFERENCE

Plaintiffs do not know the identity of the defendants, and, as such, are unable to confer.

Dated: August 3, 2017 s/Gary J. Fischman/
Gary J. Fischman

EXHIBIT 1

FISCHMAN DECLARATION

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Headhunter, LLC, *Plaintiff,* v. Does 1–17, *Defendants*.	§ § § § § § § § § § § §	Case No. 4:17-cv-2352 Jury

DECLARATION OF GARY J. FISCHMAN IN SUPPORT OF PLAINTIFF'S *EX PARTE* MOTION FOR EXPEDITED DISCOVERY

I, Gary J. Fischman, declare:

¶1. I am over the age of 18, this declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

¶2. Maverickeye UG ("Maverickeye"), a company organized and existing under the laws of Germany with its principal address at Heilbronner Strasse 150, 70191 Stuttgart, Germany, has surveiled Headhunter Productions, Inc.'s intellectual property within Peer-to-Peer ("P2P") networks, like BitTorrent, to identify, analyze, archive and document the distribution of the movie A Family Man ("Motion Picture").

¶3. I have reviewed the collected records and verified that the surveillance software identified the IP addresses listed in Exhibit 2 of the Complaint as distributing and making available a copy of the Motion Picture having the unique hash identifier

66142306B49AA8486978898BA51B7273A3B85327

at the listed date and times via a P2P network.

¶4. Further, the identified IP addresses copying, distributing, and making available plaintiff's Motion Picture geolocate, at the time those activities took place, as originating in what I understand is the Southern District of Texas.

¶5. I confirmed that the file having the unique hash number given above is promoted on the internet as corresponding to a complete copy of the Motion Picture.

¶6. While the software has captured the IP addresses, I do not have any way to determine the names, residential addresses, e-mail addresses, or any other identifying information to locate the persons associated with the IP addresses.

Per 28 U.S.C § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on: August 3, 2017 s/Gary J. Fischman/
Gary J. Fischman

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Headhunter, LLC, *Plaintiff,* v. Does 1–17, *Defendants*.	§ § § § § § § § § § § § §	Case No. 4:17-cv-2352 Jury

ORDER RE PLAINTIFF HEADHUNTER LLC'S *EX PARTE* MOTION TO TAKE PRE-26(F) CONFERENCE DISCOVERY OF THIRD-PARTY INTERNET SERVICE PROVIDER

THIS CAUSE came before the Court upon plaintiff Headhunter LLC's *ex parte* motion to take pre-26(f) conference discovery of internet service provider AT&T. The Court concludes that plaintiff's motion and supporting exhibits establish good cause for the expedited and limited discovery requested.

Accordingly, it is hereby

ORDERED that Plaintiff's Motion is **GRANTED**. It is therefore

FURTHER ORDERED that:

1. Pursuant to Federal Rule of Civil Procedure 45, Headhunter may serve a subpoena on ISP AT&T for information concerning each of the subscribers whom AT&T assigned the IP addresses referenced in Exhibit 2 of the Complaint [Doc. # 1] to plaintiff's motion.

2. The subpoenaed ISP shall not require plaintiff to pay a fee in advance of providing the subpoenaed information or for the ISP's costs to notify its customers. However, plaintiff must promptly reimburse AT&T for reasonable costs incurred in producing the material requested in the subpoenas, provided that AT&T must provide plaintiff a detailed invoice setting out the work performed.

3. If AT&T or any subscriber declines to comply with a subpoena issued pursuant to this Order, the objector must file a motion to quash before the return date of the subpoena, which will be at least 30 days from the date of service.

4. AT&T must preserve all subpoenaed information pending the resolution of a timely-filed motion to quash.

5. Any information disclosed to plaintiff in response to a subpoena may be used by plaintiff solely for the purpose of protecting plaintiff's rights as set forth in the Complaint in this case.

6. Plaintiff shall attach a copy of this Order to the subpoena.

Signed at Houston, Texas on _____, 2017.

_____
United States District Judge

APPENDIX

Page

TAB **CASE**

A *Garrett v. Comcast Comms., Inc.*,
No. 3:04-cv-693 (N.D. Tex. July 23. 2004) .....*App. 1*

B *W. Coast Prods., Inc. v. Does 1-351*,
No. 4:12-cv-00504, 2012 WL 2577551 (S.D. Tex. July 3, 2012) .....*App. 3*

C *Well Go USA, Inc. v. Unknown Participants*,
No. 12-cv-00963, 2012 WL 4387420 (S.D. Tex. Sept. 25, 2012) .....*App. 7*

DIANE GARRETT, Plaintiff,

v.

COMCAST COMMUNICATIONS, INC. Defendant.

No. 3:04-CV-693-P

United States District Court, N.D. Texas, Dallas Division.

July 23, 2004

MEMORANDUM OPINION AND ORDER

JORGE SOLIS, District Judge.

Now before the Court is Plaintiff's Motion to Remand, filed April 28, 2004. Defendant filed its Response on May 18, 2004 and Plaintiff filed its Reply on June 1, 2004. After considering the parties' arguments and briefing, and the applicable law, the Court DENIES Plaintiff's Motion to Remand.

I. Background and Procedural History

Plaintiff Diane Garrett originally filed suit in the 44th Judicial District in Dallas County, Texas on March 1, 2004. (Pl.'s Mot. to Remand at 1.) In *Diane Garrett v. Comcast Communications, Inc.*, Case No. 04-01660-B, Plaintiff alleged that Defendant, her internet service provider, released her personal information to the Recording Industry Association of America ("RIAA"), who subsequently brought suit against Plaintiff. (Compl. at 1-2.) Plaintiff claims that Defendant's actions were in violation of its published privacy policy, which states that it will not release private information provided by its consumers unless presented with a valid subpoena, and that the subpoena issued was invalid under 17 U.S.C. § 512(h) (2004). (Compl. at 2-3.; Pl.'s Appendix, Ex. A, p. 3.) As a result, Plaintiff claims that she suffered a loss of privacy, loss of private use of her residential internet service, severe humiliation, embarrassment, fear, frustration, and emotional distress, and has been forced to defend herself in a lawsuit. (Compl. at 2.) Plaintiff alleged causes of action for invasion of privacy, breach of contract, false misrepresentation, and intentional infliction of emotional distress. (Compl. at 3.) Plaintiff is suing for actual damages in excess of $1, 000, exemplary damages, post-judgment interest as provided by law, reasonable attorney's fees and costs of suit, and any other relief plaintiff is entitled to. (Compl. at 3-4.)

Defendant Comcast Communications, Inc. removed this action to the Northern District of Texas on April 2, 2004, on the basis of federal question jurisdiction, under 28 U.S.C. § 1331 (2004), or, alternatively, on the basis of diversity jurisdiction, under 28 U.S.C. § 1332(a) (2004). (Def.'s Notice of Removal at 1-2; Pl.'s Mot. to Remand at 2.)

II. Motion to Remand

Removal of a state court action to federal court is proper when the complaint falls within the original subject-matter jurisdiction of the federal district court. *See* 28 U.S.C. § 1441(a) (2004). A court of the United States has original subject matter jurisdiction of a dispute if it arises under the Constitution, laws, or treatises of the United States. 28 U.S.C. § 1331; *see also O'Quinn v. Manuel*, 773 F.2d 605, 607 (5th Cir. 1985). "In determining whether a claim arises under federal law, the Court must look to the well-pleaded complaint, ' not the removal petition." *Nelon v. Mitchell Energy Corp.*, 941 F.Supp. 73, 74 (N.D. Tex. 1996) (citing *Merrell Dow Pharmaceuticals, Inc. v. Thompson*, 478 U.S. 804, 808 (1986); *Willy v. Coastal Corp.*, 855 F.2d 1160, 1165 (5th Cir. 1988)). Federal-question jurisdiction exists where federal law creates the cause of action; however, it may also exist "where the vindication of a right under state law necessarily turn[s] on some construction of federal law." *Id.* (quoting *Merrell Dow*, 478 U.S. at 808). The burden of establishing that federal jurisdiction exists lies with the removing party. *See St. Paul Reinsurance Co., Ltd. v. Greenburg*, 134 F.3d 1250, 1253 (5th Cir. 1998).

Plaintiff's claims for invasion of privacy, breach of contract, false misrepresentation, and intentional infliction of emotional distress are premised on her allegation that Defendant released her records without a valid subpoena, under 17 U.S.C. § 512(h). (Compl. at 2-3.) If the subpoena issued to Defendant by RIAA was valid, Defendant's actions were within the terms of its privacy policy, which clearly states that it will release customer information if presented with a valid subpoena. (Pl.'s App. at Ex. A, p. 3.) Therefore, the threshold question to be addressed by the Court is whether the subpoena is valid under 17 U.S.C. § 512(h).[1] Because the vindication of Plaintiff's state law rights turns on the construction of a federal statute, federal question jurisdiction exists. *See Nelon*, 941 F.Supp. at 74 (quoting *Merrell Dow*, 478 U.S. at 808).[2]

III. Conclusion

For the reasons set forth above, the Court finds that Defendant has satisfied its burden of establishing that the Court has subject matter jurisdiction over Plaintiff's claims. Accordingly, the Court DENIES Plaintiff's Motion to Remand.

IT IS SO ORDERED.

Notes:

[1] Plaintiff claims that the subpoena was already declared invalid in *Recording Indus. Ass'n of America, Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229 (D.C. Cir. 2003), and the only remaining issues for the court to decide are Plaintiff's state law claims. (Pl.'s Memorandum in Supp. of Mot. to Remand at 2.) However, *RIAA v. Verizon* held that a subpoena issued under § 512(h) was valid if it was issued to an internet service provider engaged in storing on its servers material that is infringing or the subject of infringing activities. 351 F.3d at 1233. Only subpoenas issued to internet service providers acting as a conduit for data transferred between two internet users, such as persons sending e-mail or "P2P" files, were declared invalid by the D.C. Circuit Court. *Id.* Plaintiff has not alleged information that would allow the Court to determine which situation was present in this case. Moreover, this Court is not bound to follow the precedent of *RIAA v. Verizon*.

[2] The Court does not reach the question of whether diversity jurisdiction exists in this case because it has already found federal question subject matter jurisdiction.

WEST COAST PRODUCTIONS, INC., Plaintiff,

v.

DOES 1-351, Defendants.

Civil Action No. 4:12-CV-00504

United States District Court, S.D. Texas, Houston Division.

July 3, 2012

MEMORANDUM AND ORDER

NANCY F. ATLAS, District Judge.

I. BACKGROUND

On February 20, 2012, Plaintiff filed a Complaint [Doc. # 1] against 351 unnamed Doe Defendants identified in the Complaint solely by their Internet protocol ("IP") addresses and Internet Service Providers ("ISP"). *See* Ex. A to Compl. [Doc. # 1-1]. Plaintiff alleges that these Doe Defendants infringed Plaintiff's copyright for the adult video "Monster Wet Anal Asses" ("Video"), registered with the Copyright Office on October 18, 2011.[1] *See* Compl., ¶¶ 3, 25. Subsequently, Plaintiff filed an Unopposed Motion for Expedited Discovery [Doc. # 3] seeking leave to serve third-party subpoenas prior to a Rule 26(f) conference. The Court granted Plaintiff's Motion on February 28, 2012, *see* Order [Doc. # 5], but modified Plaintiff's Proposed Order [Doc. # 3-2] to (1) limit the issuance of subpoenas to only those ISPs identified in Exhibit A to the Complaint; (2) require that Plaintiff serve copies of all materials and information obtained from an ISP about any individual putative Doe Defendant on that specific individual; and (3) require that ISPs send all affected subscribers a notice ("Notice') stating that the individual had "30 days from the date of this notice to file a motion to quash or vacate the subpoena." *See* Order [Doc. # 5], ¶¶ 1, 2, 5; App'x A to Order [Doc. # 5-1].

Subsequently, individuals identified as Doe Defendants # 3, # 36, # 123, # 328, and # 342 filed Motions to Dismiss, Sever, Quash, Modify, and/or for Protective Order. *See* Motions [Docs. ## 8, 9, 13, 17, 20]. The Movants make similar arguments (1) that joinder is improper because they were not part of the same transaction or occurrence, (2) that the Court lacks personal jurisdiction over this case, and (3) that the subpoenas should be quashed because they invade their privacy and/or impinge on their First Amendment right to anonymous speech, or because they subject Movants to undue burden. Plaintiff responded to each Motion. *See* Pl. Resps. [Docs. ## 18, 19, 21, 26, and 28]. No Defendant filed a reply. At the initial pretrial conference on May 16, 2012, the Court heard oral argument on the Motions, which are now ripe for decision.

II. RULE 11 REQUIREMENTS FOR MOTIONS

"Every pleading, written motion, and other paper must be signed by at least one attorney of record in the attorney's name-or by a party personally if the party is unrepresented. The paper must state the signer's address, e-mail address, and telephone number." FED. R. CIV. P. 11(a). The purpose of Rule 11 is to maintain the integrity of the system of federal practice and procedure, deter baseless filings, and streamline the administration and procedure of federal courts. *See Malibu Media, LLC v. Does 1-13*, No. CV 12-1156, 2012 WL 2325588, at *2 (E.D.N.Y. June 19, 2012) (Boyle, Magistrate J.); *Pink Lotus Entm't, LLC, v. Does 1-53*, No. 11-22103 [Doc # 19] (S.D. Fla. Sept. 6, 2011) (Seitz, J.); *Hard Drive Prods., Inc. v. Does 1-21*, 4:11-cv-0059 [Docs. # 22, 35, 36] (S.D. Ind. July 27, 2011) (Barker, J.); *see also Bus. Guides, Inc. v. Chromatic Commc'n Enters., Inc.*, 498 U.S. 533, 541-43 (1991) (discussing the purposes of Rule 11).

On April 13, 2012, an individual using the name "John Doe # 3" and the email address *johndoes1.351@gmail.com* filed a *pro se* Motion to Sever and/or Quash. *See* Motion [Doc. # 8]. The Motion did not identify the filer's actual name. *See id.* at 14-15. Because the Court must be informed as to the identities of the parties before it and the purported Doe # 3 has not provided the requisite Rule 11(a) information, the Court cannot permit this individual to litigate here.[2] Doe # 3's Motion is denied on this basis.

The remaining Movants also fail to identify their names in their Motions. *See* Motions [Docs. ## 9, 13, 17, 20]. Unlike Doe # 3, however, the other Movants either notified the Court of their identities under seal and/or are represented by counsel admitted to the Bar of this Court. These represented parties' attorneys have well-established professional duties of candor to the Court, which duties protect against unauthorized filings or participation in this suit by persons whose information Plaintiff did not attempt to subpoena. The Court will permit Doe Defendants # 36, # 123, # 328, and # 342 to remain anonymous in the public record for purposes of the pending motions. *See infra* Section VI.

III. MOTION TO DISMISS OR SEVER FOR IMPROPER JOINDER

Rule 20 of the Federal Rules of Civil Procedure permits joinder of defendants if (1) "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 (2) "any question of law or fact common to all defendants will arise in the action." FED. R. CIV. P. 20(a)(2). Because the purpose of Rule 20 is to facilitate trial convenience and expedite the resolution of disputes, thereby eliminating unnecessary lawsuits, district courts should liberally construe permissive joinder of claims and parties in the interest of judicial economy. *Klein Indep. School Dist. v. Hovem*, No. H-09-137, 2010 WL 1068076, at *4 (S.D. Tex. Mar. 22, 2010) (Harmon, J.) (citing *United Mine Workers v. Gibbs*, 383 U.S. 715, 724 (1966) ("Under the Rules, the impulse is towards entertaining the broadest possible scope of action consistent with fairness to the parties; joinder of claims, parties and remedies is strongly encouraged.")); *see also Acevedo v. Allsup's Convenience Stores, Inc.*, 600 F.3d 516, 521 (5th Cir. 2010).

Rule 21 further provides that "[m]isjoinder of parties is not a 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." FED. R. CIV. P. 21. Because Rule 21 does not provide a specific standard by which courts can determine if parties are properly joined, courts often look to Rule 20 for guidance. *See Acevedo*, 600 F.3d at 521.

The Movants argue that they should be dismissed or severed because they were improperly joined. The Court is unpersuaded. The present record provides *prima facie* evidence that the alleged BitTorrent activity regarding the Defendants is part of the same transaction and occurrence. *See, e.g., Patrick Collins v. Does 1-21*, No. 11-15232, 2012 WL 1190840, at *5-*10 (E.D. Mich. Apr. 5, 2012) (Randon, Magistrate J.); *First Time Video, LLC v. Does 1-76*, 1:11-cv-03831 [Doc. # 38], at *3 (N.D. Ill. Aug. 16, 2011) (Bucklo, J.); *Voltage Pictures, LLC v. Does 1-5000*, No. 10-0873, 2011 WL 1807438, at *4 (D.D.C. May 12, 2011) (Howell, J.). *But see K-Beech, Inc. v. Does 1-41*, No. V-11-46, 2012 WL 773683, at *3 (S.D. Tex. Mar. 8, 2012) (Rainey, J.) (collecting cases holding otherwise). In its Complaint, for example, Plaintiff alleges that "[i]n using the peer-to-peer BitTorrent file distribution method, each Defendant engaged in a concerted action with other Defendants and yet unnamed individuals to reproduce and distribute Plaintiff's Video by exchanging pieces of the Video file in the torrent swarm." Doc. # 1, ¶ 33. This allegation is supported by an affidavit attached to Plaintiff's Motion for Expedited Discovery, in which the affiant states that "each of the participating peers obtained a reference file for Plaintiff's copyrighted film, " that "each reference file has a unique identifier, " and that "the swarm [that] each of the peers participated in is associated with the... unique identifier." *See* Aff. [Doc. # 3-1], ¶¶ 9, 11.

For purposes of the pending motions, Plaintiff has also established that there are various common questions of law and fact that appear to pertain to all Defendants. For instance, the Court will need to determine whether copying has occurred within the meaning of the Copyright Act, whether entering and/or remaining in a torrent swarm constitutes a willful act of infringement or civil conspiracy, and whether and to what extent Plaintiff has been damaged by one or more Defendants' conduct. *See* Compl. ¶ 8.

Plaintiff now merely seeks identifying information in order to investigate the facts concerning, to formally name, and to serve a subset of currently referenced Doe Defendants if in fact the individuals have a provable connection to the swarm identified in this suit.[3] It is significantly more efficient *at this phase* for the Court and Plaintiff to maintain a single case with a large number of Defendants to be further investigated for their putative connection to the swarm at issue, rather than hundreds of separate lawsuits. *See, e.g., Call of the Wild Movie, LLC v. Does 1-1062*, 770 F.Supp.2d 332, 344 (D.D.C. Mar. 22, 2011) (Howell, J.). If Plaintiff proceeds in this action or elsewhere against specific named Defendants, those Defendants may raise applicable joinder issues at that time. It may well be unwieldy to have one case with hundreds of defendants with differing explanations for their connections to the IP addresses identified by Plaintiff, but the Court does not reach that issue now. *See, e.g., K-Beech, Inc. v. Does 1-41*, 2012 WL 773683, at *5; *AF Holdings v. Does 1-97*, No. C 11-3067, 2011 WL 5195227, at *3 (N.D. Cal. Nov. 1, 2011) (Wilken, J.). Doe Defendants' Motions to Dismiss or Sever are therefore denied at this time.

IV. MOTION TO DISMISS FOR LACK OF PERSONAL JURISDICTION

Doe Defendants # 328 and # 342 argue that they should be severed or dismissed because the Court lacks personal jurisdiction over them.[4] *See* Doc. # 13, ¶ 9; Doc. # 20, ¶ 3. The Court does not decide this issue here. Analysis of personal jurisdiction is premature when Plaintiff has not identified and named the Defendants against whom claims in fact will be asserted. The current record is plainly inadequate on the personal jurisdiction issue. *See, e.g., First Time Video*, LLC v. Does 1-76, No. 1:11-cv-03831 [Doc. # 38], at *11 (N.D. Ill. Aug. 16, 2011) (Bucklo, J.); *First Time Videos, LLC v. Does 1-500*, No. 10-CV-6254 [Doc. # 151], at *17 (N.D. Ill. Aug. 9, 2011) (Castillo, J.); *Hard Drive Prods. v. Does 1-46*, No. 3-11-cv-01959 [Doc. # 19], at *1 (N.D. Cal. June 16, 2011) (Chen, J.); *Call of the Wild Movie, LLC v. Does 1-1062*, 770 F.Supp.2d 332, 346-348 (D.D.C. Mar. 22, 2011) (Howell, J.); *IO Group v. Does 1-19*, No. C 10-03851, 2010 WL 5071605, at *3 (N.D. Cal. Dec. 7, 2010) (Illston, J.). Plaintiff is directed, however, that it must have a good faith factual basis for this Court to assert personal

jurisdiction over each Defendant Plaintiff pursues in this suit on the merits.

V. MOTION TO QUASH AND PRIVILEGE ISSUES

"On timely motion, the issuing court must quash or modify a subpoena that... requires disclosure of privileged or other protected matter, if no exception or waiver applies, ... [or that] subjects a person to undue burden." FED. R. CIV. P. 45(c)(3)(A). Under other limited circumstances, the "issuing court may, on motion, quash or modify the subpoena...." *Id.* § 45(c)(3)(B).

Movants argue that their Motion to Quash should be granted because the subpoenas invade their privacy and/or impinge on their First Amendment right to anonymous speech. The Court is unpersuaded. Plaintiff contends, with some supporting affidavit evidence, that the BitTorrent swarm tied to the Video infringes its copyright in a protected work identified by the Video's digital reference file. Plaintiff is entitled to seek to assert its legal claims against persons shown to have willingly become a part of the BitTorrent swarm associated with that digital reference file. This is not the stage for legal rulings on the viability of the contention that swarm participants have engaged in violations of the copyright laws. To the extent that anonymity is used to mask copyright infringement or to facilitate such infringement by others, the First Amendment is no protection. *See, e.g., Arista Records LLC v. Does 1-16,* 604 F.3d 110, 118-119 (2d Cir. 2010) (citing *Sony Music Entm't, Inc. v. Does 1-40,* 326 F.Supp.2d 556, 563-565 (S.D.N.Y. 2004) (Chin, J.) (identifying expectation of privacy as one of five factors to consider in evaluating a party's First Amendment interest in protecting their identity from disclosure)); *Nu Image, Inc. v. Does 1-3932,* 2:11-CV-545-FTM-29, 2012 WL 646070, at *6 (M.D. Fla. Feb. 28, 2012) (Chappell, J. Magistrate); *MCGIP, LLC v. Does 1-316,* No. 10 C 6677, at *1-*2 (N.D. Ill. June 9, 2011) (Kendall, J.). The Court rejects the Movants' First Amendment and privacy arguments attempting to quash the subpoenas in issue here.

The Movants also argue that the subpoenas subject them to undue burden because the information sought is irrelevant or inaccurate. The Court again is unpersuaded. It is true that IP addresses cannot pinpoint a person responsible for a particular file download and IP address-tracing technologies are not always reliable. *See, e.g., SBO Pictures, Inc. v. Does 1-3036,* No. 11-4220, 2011 WL 6002620, at *3 (N.D. Cal. Nov. 30, 2011) (Conti, J.). Nevertheless, it is reasonable to use an IP address as a starting point to obtain identifying information about a Doe Defendant who, through digital forensic means, has been tied to the torrent swarm in issue. The identifying information allows Plaintiff to make a good faith investigation into whether a particular individual has a reliable factual connection to the IP address associated with the swarm. If Plaintiff learns that the IP address is not a reliable identifier for a person, who Plaintiff in good faith can show committed an alleged legal wrong, Plaintiff has an obligation under Federal Rule of Civil Procedure 11 to cease pursuit of the claim against that individual. Plaintiff's counsel at a pretrial conference and at oral argument expressly committed that for each IP address, Plaintiff will assess whether pursuit of claims against each Defendant in fact is warranted once the individual associated with the IP address has been identified.

The Movants also attempt to argue the merits of the case by asserting that the subpoenas unduly burden them because they did not in fact infringe Plaintiff's work. This argument lacks merit. Being named a defendant in this type of case does not in and of itself constitute an undue burden to warrant quashing a subpoena. *See, e.g., Hard Drive Prods. v. Does 1-46,* No. 3-11-cv-01959 [Doc. # 19], at *2 (N.D. Cal. June 16, 2011) (Chen, J.). "[T]he merits of this case are not relevant to the issue of whether the subpoena is valid and enforceable." *See, e.g., Achte/Neunte Boll Kino Beteiligungs GMBH & Co. Kg. v. Does 1-4577,* No. 10-453, 736 F.Supp.2d 212, 215 (D.D.C. 2010) (Collyer, J.). Accordingly, the Doe Defendants' Motions to Quash are denied.

VI. MOTION FOR PROTECTIVE ORDER

"The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense...." FED. R. CIV. P. 26(c)(1). Here, Does # 123 and # 328 seek a protective order prohibiting the public disclosure of any information relating to him or her that is obtained via the subpoena, *see* Motion [Doc. # 13], at 1, 12; allowing "information regarding the Defendant's identity to remain sealed and confidential, " *see* Motion [Doc. # 17], at 4; or preventing Plaintiff from using the subpoenaed information "to harass, embarrass or expose the [Defendant] to undue burden, " *see id.* at 6.

Movants are not the respondents on Plaintiff's subpoenas. The Court recognizes, however, that being accused in a publicly filed lawsuit as a participant in the copyright infringement of an adult video poses the risk of embarrassment. Because this is an early stage in the proceedings, and because Plaintiff has little information about the Doe Defendants' connection to the IP addresses at which the allegedly infringing activity occurred, the Court concludes that there is good cause to protect from public disclosure at this time any identifying information produced under the subpoenas. *See IO Group v. Does 1-19,* No. C 10-03851, 2010 WL 5071605, at *2 (N.D. Cal. Dec. 7, 2010) (Illston, J.). The Court therefore will grant a limited

protective order prohibiting Plaintiff from filing in the public record (or otherwise disclosing outside this suit) any subpoenaed information about a Doe Defendant's identity until the affected Defendant has a reasonable opportunity to move to proceed anonymously and the Court has ruled on the motion. A reasonable opportunity is deemed to be thirty days after either his or her personal information is disclosed by an ISP to Plaintiff or after the date of this Order, whichever is later. In the absence of a timely motion or Plaintiff's agreement to maintain a Doe Defendant's confidentiality, this limited protective order will expire. To the extent that any Doe Defendant seeks to prevent an ISP from disclosing identifying information to Plaintiff, however, the motion is denied.

VII. CONCLUSION

For the foregoing reasons, it is hereby

ORDERED that Doe # 3's Motion to Sever and/or Quash [Doc. # 8] is DENIED. It is further

ORDERED that Doe # 36's Motion to Quash, Dismiss, or Sever [Doc. # 9] is DENIED. It is further

ORDERED that Doe # 328's Motion to Sever, Quash, or Modify Subpoena [Doc. # 13] is DENIED in part and GRANTED in part. It is further

ORDERED that Doe # 123's Motion to Dismiss, Sever, Quash, and for Protective Order [Doc. # 17] is DENIED in part and GRANTED in part. It is further

ORDERED that Doe # 342's Motion to Quash, Dismiss, or Sever [Doc. # 20] is DENIED.

Notes:

[1] The Registration Number for the work is PA X-XXX-XXX. *See* Ex. B to Compl. [Doc. # 1-2].

[2] According to Plaintiff, the Motion filed purportedly by Doe # 3 is also problematic because Plaintiff never subpoenaed Cable One, the ISP associated with Doe # 3 in Exhibit A to Plaintiff's Complaint. *See* Pl. Filing [Doc. # 25], ¶ 1. In its Motion, purported Doe # 3 appears to identify his ISP as Comcast Cable Communications, LLC ("Comcast"). Comcast, however, is not the ISP associated with Doe # 3 listed in the Complaint. *Compare* Motion [Doc. # 8] (certifying that Doe # 3's Motion was faxed to Comcast) *with* Ex. A. to Complaint [Doc. # 1-1] (identifying Cable One as the ISP associated with Doe # 3). This inconsistency casts doubt on whether the Motion regarding Doe # 3 was in fact filed by Doe # 3. Also, no one identifying himself as Doe # 3 appeared in person or by phone at the May 16, 2012 initial pretrial conference in this case, despite this Court's order that "all persons or counsel of persons with pending motions" in this case must appear at the conference. *See* Order [Doc. # 22]. The Court's inability to confirm whether the Motion filed by Doe # 3 is in fact a communication from the Doe # 3 listed in the Complaint is emblematic of the problems against which Rule 11 protects.

[3] *See infra* page 11.

[4] Doe # 342 also filed a list of the geographic locations associated with the 351 IP addresses identified in Exhibit A. *See* Ex. D to Motion [Doc. # 20-4]. According to Doe # 342, these lists were generated using two different online IP look-up tools. *See* Motion [Doc. # 20], ¶ 16. The list contains a not insignificant number of IP addresses associated with users in districts other than the Southern District of Texas.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

WELL GO USA, INC. A TEXAS CORPORATION,	§	
	§	
Plaintiff,	§	
v.	§	**CIVIL ACTION NO. 4:12-cv-00963**
	§	
UNKNOWN PARTICIPANTS IN FILESHARING SWARM IDENTIFIED BY HASH: B7FEC872874D0CC9B1372ECE5ED07AD7420A3BBB,	§	
	§	
Defendants.	§	

MEMORANDUM & ORDER

Before the Court is Plaintiff's Motion for Leave to Identify Defendants (Doc. No. 8) relating to the alleged copyright infringement of Plaintiff's movie, "Ip Man 2". Specifically, Plaintiff seeks the names of those it believes used BitTorrent technology to illegally share Ip Man 2. Based on Plaintiff's Motion and the applicable law, this court grants limited discovery.

I. BACKGROUND

BitTorrent is a peer-to-peer ("P2P") file sharing protocol used for distributing and sharing data on the Internet. Unlike other P2P protocols, BitTorrent downloading occurs through a piecemeal process by which a user can receive different portions of the file from multiple users. As soon as a user has downloaded a new piece of the file, she or he becomes able to transmit that piece to other peers. All peers who have a common BitTorrent file on their computer are considered a single "swarm." A swarm is identified by a unique hash tag, which Plaintiff identified in its complaint as "B7FEC872874D0CC9-

B1372ECE5ED07AD7420A3BBB." As long as users are connected to the BitTorrent protocol, they continue to distribute data to the peers in the swarm until the user manually disconnects from the swarm or the computer is shut down. *Diabolic Video Prods., Inc. v. Does 1–2099*, 2011 WL 3100404, *1–2 (N.D.Cal. May 31, 2011) cited by *K-Beech, Inc. v. John Does 1-41*, CIV.A. V-11-46, 2012 WL 773683 (S.D. Tex. Mar. 8, 2012).

Plaintiff attempts to join all Does who participated in the swarm from May 10, 2011 to July 15, 2011. (Compl. ¶ 12.) During this time, Plaintiff obtained each subscriber's IP address, the specific internet service provider (ISP), and the date and time of the infringing activity. (Doc. No. 8-3.) Plaintiff acknowledges that all Defendants did not engage with the swarm at the exact same time. (Doc. No. 8, at 7.)

Plaintiff requests leave of the court to identify each Defendant's name, address, telephone number, and email address. Plaintiff desires to use the subpoena provision of the Digital Millennium Copyright Act to compel ISPs to release Defendants' information. 17 USC § 512(h). In the alternative, Plaintiff requests permission to serve Rule 45 subpoenas on the ISPs. This Court grants limited discovery under Rule 45, subject to the protective order below.

II. ANALYSIS

A. Validity of Subpoena for Identifying Information

In order to seek a subpoena for identifying information of users, courts have weighed several factors to balance the need for disclosure against First Amendment interests. These factors include: (1) a concrete showing of a prima facie claim of actionable harm by the plaintiff; (2) specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) a central need for the subpoenaed

information to advance the claim; and (5) the user's expectation of privacy. *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 114 (2d Cir. 2010) citing *Sony Music Entm't Inc. v. Does 1-40*, 326 F.Supp.2d. 556, 565 (S.D.N.Y. 2004). *See also Call of the Wild Movie, LLC v. Does 1-1,062*, 770 F. Supp. 2d 332, 350 (D.D.C. 2011); *Interscope Records v. Does 1-14*, 558 F. Supp. 2d 1176, 1179 (D. Kan. 2008); *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 164 (D. Mass. 2008).

Plaintiff has asserted a prima facie claim for copyright infringement. Plaintiff's Complaint alleges that Plaintiff is the owner of Ip Man 2 and that Defendants downloaded Ip Man 2 without Plaintiff's authorization. Plaintiff claims that once this file was downloaded, it was a complete and accurate embodiment of Ip Man 2. Plaintiff has also provided the IP addresses of the individuals who were participating in the swarm and downloading the movie file illegally. (Doc. No. 8-3.) Plaintiff's complaint, along with the IP addresses, demonstrate a prima facie case (factor 1) and also demonstrate specificity (factor 2).

Plaintiff also must show that there is no alternate means to obtain the information (factor 3). Plaintiff states in its Motion that it has "obtained all information it possibly can without discovery from the service providers." Without expedited discovery to uncover Defendants' identifying information, the Court finds that Plaintiff cannot proceed. Plaintiff has also fulfilled factor 4, demonstrating a central need for the identifying information of Defendants. Plaintiffs cannot serve Defendants without knowing their identifying information, nor can Defendants respond to Plaintiff's allegations.

In terms of Defendants' expectation of privacy, under the protective order, Defendants will have a chance to object and respond to Plaintiff's claims, and will have a

chance to contest the subpoena before their names are turned over to Plaintiff. Thus, their information will remain private during the Court's determination of any motions that ISPs or Defendants wish to file (including a motion to quash, or to proceed anonymously). Thus, the Court believes that Defendants' First Amendment rights to anonymity do not prevent disclosure of identifying information.

B. Copyright Act Subpoena versus Rule 45 Discovery

Plaintiff seeks to identify Defendants under the Digital Millennium Copyright Act. 17 USC § 512(h). The first and most significant decision to interpret the extent of the subpoena authority of 512(h) was *Recording Industry Ass'n of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003). The *Verizon* court held that 512(h) authorized subpoenas only for ISPs that were actually storing infringing material, not simply acting as conduits for the material. In P2P protocols such as BitTorrent, ISPs do not generally store any infringing material. The material is located on users' computers (or in an off-line storage device, such as a compact disc), not on the ISP computers. *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc*., 351 F.3d 1229, 1235 (D.C. Cir. 2003).

Looking at both the language and the structure of the Act, the *Verizon* court rested its decision, in the main, on the text of 512(h) in relation to another subsection, 512(c)(3)(A). The court found that 512(h) required that subpoenas contain "a copy of a notification described in subsection [512](c)(3)(A)." *Verizon*, 351 F.3d at 1234. The notification provision of 512(c)(3)(A) "is found within one of the four safe harbors created by the statute to protect ISPs from liability for copyright infringement under certain

conditions." *In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 775 (8th Cir. 2005). Each safe harbor applies to a particular ISP function. The first safe harbor, under § 512(a), limits the liability of ISPs when they do nothing more than transmit, route, or provide connections for copyrighted material—that is, when the ISP is a mere conduit for the transmission. *Id.* Thus, a copyright owner cannot request a subpoena for an ISP which merely acts as a conduit for data.

Each of the other three safe harbors protects the ISP from liability if the ISP responds expeditiously to remove or disable access to infringing material. These three safe harbors require the ISP to be able both to locate and remove the infringing material, as a way of allowing the ISP to protect itself from liability. However, with P2P file sharing, the file itself is on the user's system and cannot be located or removed by the ISP.

Thus, the safe harbor implicated here, 512(a), limits the liability of an ISP when it merely acts as a conduit for infringing material. A number of other courts have read 512(h) in a similar manner. *In re Charter Communications*, 393 F.3d at 773; *In re Subpoena To Univ. of N. Carolina at Chapel Hill*, 367 F. Supp. 2d 945, 952 (M.D.N.C. 2005); *Interscope Records v. Does 1-7*, 494 F. Supp. 2d 388, 391 (E.D. Va. 2007). While this Court acknowledges it is not bound to follow the precedent of *Verizon*, it finds compelling the statutory analysis employed in *Verizon*.

Plaintiff lists nine ISPs in its Motion, but does not allege that all ISPs were storing infringing material on their servers (rather than merely acting as conduits). Plaintiff claims that Defendants using Verizon *may* have stored, shared, and viewed documents on Verizon's own servers. (Doc. No. 11.) However, there are eight other ISPs that were used by Doe Defendants. Because of the nature of P2P activity, these ISPs were likely used only

as conduits to download any infringing material. Thus, these ISPs likely fall within the safe harbor described in 512(a) and discovery should be granted through a different mechanism if possible.

Discovery can be granted under Rule 45 to obtain Defendants' identifying information, subject to a protective order. The protective order—issued under Rule 26(c)(1) of the Federal Rules of Civil Procedure—will allow the Doe Defendants and the ISPs to be heard before identifying information is released to Plaintiff. *See Hard Drive Productions, Inc. v. Does 1-59*, CIV.A. H-12-0699, 2012 WL 1096117 (S.D. Tex. Mar. 30, 2012); *Digital Sin, Inc. v. Does* 1-176, 279 F.R.D. 239, 242 (S.D.N.Y. 2012).

C. Joinder

The Court is also concerned as to whether Defendants are properly joined under Fed. R. Civ. P. 20(a). Courts are split on the question of whether a swarm of users can be joined in a single case. The Court recognizes that, while the Defendants participated in the same swarm in downloading Ip Man 2, this may not be considered the same transaction or occurrence, or the same series of transactions or occurrences. *Liberty Media Holdings, LLC v. BitTorrent Swarm*, 277 F.R.D. 669 (S.D. Fla. 2011); *CineTel Films, Inc. v. Does 1-1,052*, 853 F. Supp. 2d 545 (D. Md. 2012); *Patrick Collins, Inc. v. John Does 1–23*, 11–CV–15231, 2012 WL 1019034 (E.D.Mich. Mar. 26, 2012); *Hard Drive Prods., Inc. v. Does 1–30*, 2011 WL 4915551, at *4 (E.D.Va. Oct. 17, 2011); *Hard Drive Productions, Inc. v. Does 1-188*, 809 F. Supp. 2d 1150, 1156 (N.D. Cal. 2011). *But see Hard Drive Prods., Inc. v. Does 1–55*, 2011 WL 4889094, at *5 (N.D.Ill. Oct. 12, 2011) (finding joinder appropriate)*; Donkeyball Movie, LLC v. Does 1–171*, 810 F.Supp.2d 20, 26–27, 2011 WL 1807452, at *4 (D.D.C. May 12, 2011) (same).

In this case, the activity of all the Defendants occurred over a ten week period. One court, considering a lesser time span of swarm activity, found that, because the activity of the defendants occurred on "different days and times over a two-week period," there was "no evidence to suggest that each of the [defendants] 'acted in concert' with all of the others." *Hard Drive Productions, Inc. v. Does 1-188*, 809 F. Supp. 2d 1150, 1164 (N.D. Cal. 2011). There are also manageability difficulties and procedural inefficiencies to consider. *Hard Drive Productions, Inc. v. Does 1-130*, C-11-3826 DMR, 2011 WL 5573960 (N.D. Cal. Nov. 16, 2011). Joinder of the more than six hundred Defendants in this case could seriously delay litigation proceedings. *Liberty Media Holdings, LLC v. BitTorrent Swarm*, 277 F.R.D. 669, 672 (S.D. Fla. 2011). Defendants may also assert different factual and legal defenses. Permitting joinder would force the Court to address the unique defenses that are likely to be advanced by each individual Defendant, creating scores of mini-trials involving differening evidence and issues. *Hard Drive Prods., Inc.*, 809 F.Supp.2d at 1164.

On the other hand, Defendants were trading the exact same file as part of the same swarm. *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 244 (S.D.N.Y. 2012). One court considering joinder of Does over a three month period found that "each download of the file directly facilitated the others in such a way that the entire series of transactions would have been different but for each of Defendants' infringements." *Patrick Collins, Inc. v. Doe*, 2012 U.S. Dist. LEXIS 57187 (D. Md. Apr. 23, 2012).

The issue of joinder is better analyzed once unknown Defendants have been identified and served. *See MCGIP, LLC v. Does 1–18*, 2011 WL 2181620, at *1 (N.D.Cal. June 2, 2011); *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 244 (S.D.N.Y. 2012); *Hard*

Drive Productions, Inc. v. Does 1-59, CIV.A. H-12-0699, 2012 WL 1096117 (S.D. Tex. Mar. 30, 2012). After service, Defendants may present specific legal and factual defenses that would demonstrate the impropriety of permissive joinder. At this time, however, the Court finds that joinder is permissive for the purposes of carrying out the initial discovery and of gathering Defendants' identifying information in an efficient manner.

Finally, the Court notes that the relevant dates of the swarm listed on the Complaint (Compl. ¶12) are not the same as the dates that Plaintiff displayed in the Exhibits attached to its Motion. (Doc. No. 8-3.) Plaintiff alleges that the infringement started as early as April 8, 2011 and continued past July 10, 2011. However, the Court will allow discovery only for the IP addresses that were actually identified by Plaintiff's exhibit (Doc. No. 8-3). These IP addresses extend from Doe #1 on April 8, 2011 to Doe #643 on July 10, 2011.

III. PROTECTIVE ORDER

IT IS HEREBY ORDERED that Plaintiff may immediately serve Rule 45 subpoena on the ISPs listed in Doc. No. 8-1 to obtain information to identify Does 1–643, specifically her or his name, address, telephone number, and email address. The subpoena shall have a copy of this order attached.

IT IS FURTHER ORDERED that each ISP will have *60 days* from the date of service of the Rule 45 subpoena upon it to serve Does 1–643 with a copy of the subpoena and a copy of this order. Each ISP may serve Does 1–643 using any reasonable means, including written notice sent to her or his last known address, transmitted either by first-class mail or via overnight service.

IT IS FURTHER ORDERED that Does 1–643 shall have *60 days* from the date of service of the Rule 45 subpoena and this Order upon her or him to file any motions with

this Court contesting the subpoena (including a motion to quash or modify the subpoena), as well as any request to litigate the subpoena anonymously. The ISPs may not turn over the Doe Defendants' identifying information to Plaintiff before the expiration of this 60–day period and further order of the Court.

Additionally, if a Defendant or ISP files a motion to quash the subpoena, the Defendant or ISP should inform all ISPs so that the ISPs are on notice not to release any of the other Defendants' contact information until the Court rules on such motions.

IT IS FURTHER ORDERED that, if the 60–day period lapses without a Doe defendant or ISP contesting the subpoena, the respective ISPs will have 14 days to produce the subpoenaed information to Plaintiff.

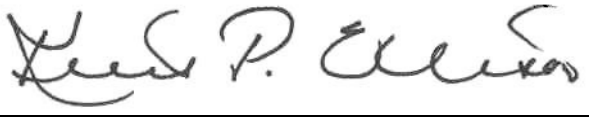
IT IS FURTHER ORDERED that ISPs must take reasonable steps to preserve the subpoenaed information pending the resolution of any timely filed motion to quash. Any ISP may file a motion to address any undue burden caused by this preservation obligation.

IT IS FURTHER ORDERED that an ISP that receives a subpoena pursuant to this order shall confer with Plaintiff, and shall not assess any charge in advance of providing the information requested in the subpoena. An ISP that receives a subpoena and elects to charge for the costs of production shall provide a billing summary and cost report to Plaintiff.

IT IS FURTHER ORDERED that any information ultimately disclosed to Plaintiff in response to a Rule 45 subpoena may be used by Plaintiff only for the purpose of protecting its rights as asserted in its complaint. The information disclosed is limited to use by Plaintiff in this litigation and may not be disclosed other than to counsel for the parties.

IT IS SO ORDERED.

SIGNED in Houston, Texas, on this the 24th day of September, 2012.



KEITH P. ELLISON
UNITED STATES DISTRICT COURT JUDGE