**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF LOUISIANA**

| | |
|---|---|
| **BKGTH PRODUCTIONS, LLC** | **CIVIL ACTION** |
| **VERSUS** | **NO: 13-5310** |
| **DOES 1-20** | **SECTION: "R" (4)** |

**ORDER**

Before the Court is Plaintiff, BKGTH Productions, LLC, ("Plaintiff") **Motion for Leave to Take Discovery Prior to Rule 26(f) Conference (R. Doc. 3)** seeking this Court to permit it to issue Rule 45 subpoenas to various internet service providers ("ISP") to determine the identities of several unidentifiable Doe defendants, who potentially infringed on their copyright. (R. Doc. 3, p. 5-6).

## I. Background

Plaintiff, a film producer and copyright holder of the motion picture "Bad Kids Go to Hell" filed a complaint in the Eastern District of Louisiana, on August 8, 2013, seeking damages and injunctive relief for alleged copyright infringement under 17 U.S.C. § 101, *et seq*. (R. Doc. 1). In its complaint, Plaintiff alleges that the unnamed "Doe Defendants" unauthorizedly acquired, transferred, copied, and freely distributed its motion picture to others by using a network called"BitTorrent protocol," which differs from the standard peer-to-peer ("P2P") file swapping networks. *Id.*

Plaintiff alleges that BitTorrent protocol provides low bandwidth, small computers with the

capability to participate in transferring large amounts of data, such as movie files across a P2P network. *Id.* Plaintiff alleges that this process operates as follows: an initial file provider elects to share a fire, called a "seed" with a BitTorrent network; other users on the BitTorrent network connect to the seed file to download a movie; as additional users knowingly join the network capable of illegally downloading the movie, each new user receives a different piece of data from each user who already downloaded the file, together comprising the whole movie. (R. Doc. 1, p. 1-2).

This system of users joining on a network and all downloading the same file is allegedly referred to as a "swarm." *Id.* at 2. The distributed nature of BitTorrent allegedly leads to a rapid viral spreading of a file throughout the users. *Id.* As more users join the swarm, the likelihood of a successful download allegedly increases, as any "seed" that has downloaded the file prior to the time a "subsequent user downloads the same file is automatically a source for the subsequent user so long as that first seed user is online at the same time" the subsequent user seeks to download the file. *Id.* Plaintiff alleges that because of the nature of these swarm downloads, every infringer is "stealing copyrighted material" from many ISP providers across the country. *Id.*

Plaintiff alleges that it engaged Crystal Bay Corporation ("CBC"), an alleged provider of online anti-conspiracy services for the motion picture industry, to monitor potential infringement activity. (R. Doc. 3, p. 9). Plaintiff alleges that CBC used "specially designed software technology" to identify infringers of Plaintiff's copyright using protocols investigated by CBC's software on P2P networks, which are allegedly connected to files of illegal versions of the Motion Picture. *Id.* at 11.

Plaintiff further alleges that once CBC's software program identifies an infringer of the Motion Picture, it obtains the IP address of a user "offering the file for download."[1] *Id.* When it is

[1]Plaintiff attached the affidavit of Darren M. Griffin, a software consultant in the technical department of CBC who testifies that all of these procedures were used by CBC to determine infringed activities.

available, CBC also allegedly obtains the user's pseudonym or network name and examines the user's publicly available directory on his or her computer for other fixes that "lexically match Plaintiff's Motion Picture." *Id.* Plaintiff also alleges that CBC downloads or "publically collects" information available about the network user that is useful in identifying the potential infringer. *Id.*

For each file downloaded, CBC allegedly downloads and records the following information: (a) the time and date at which the file or a part of the file was distributed by the user; (b) the IP address assigned to each user at the time of infringement; and, in some cases, (c) the video file's metadata (digital data about the file), such as title and file size, that is not part of the actual video content, but is attached to or contained within the digital file and helps identify the content of the file. *Id.* Plaintiff also alleges that CBC then creates evidence logs for each user and then stores all this information in a database. *Id.*

Plaintiff asserts that CBC allegedly obtains the IP address that is assigned to a user by its ISP, each time a user logs on or accesses the network, which changes with each log on, unless a user has a static IP address. *Id.* Furthermore, ISP's are allegedly assigned certain blocks or rangles of IP addresses by the "Internet Assigned Numbers Authority ("IANA") or a regional Internet registry such as the American Registry for Internet Numbers ("ARIN") which keeps track of IP addresses assigned to their subscribers at any given moment and retain such 'user logs' for a very limited amount of time, before erasing the data they contain." *Id.* at 12. These logs allegedly contain the most accurate means to connect "an infringer's identity to its infringing activity." *Id.*

Plaintiff states that the users' IP addresses are not automatically displayed on the network, nor are they aware of the "exact manner in which CBC determines a user's IP address" because it varies depending on the network being used. *Id.* However, Plaintiff contends that although the

users' IP address is not automatically visible, "any user's address is readily identifiable from the packets of publically available data being exchanged." *Id.* Through CBC's services, Plaintiff alleges that it realized alleged copyright infringement, as it traced the internet protocol of each of the Doe defendants to a "point of origin within the Eastern District of Louisiana." *Id.*

Shortly after filing this action, Plaintiff filed a Motion for Leave to Take Discovery Prior to Rule 26(f) Conference on September 3, 2013, seeking an Order from this Court permitting it to take discovery, namably to issue Rule 45 subpoenas to various internet service providers ("ISP") prior to the Rule 26(f) conference, to determine the identities of several unidentifiable "Doe Defendants" (R. Doc. 3, p. 5). In support of its motion, Plaintiff argued that precedent allowed for expedited discovery, and that it has shown good cause for said discovery. *Id.* at 2.

Prior to issuing a ruling on said motion, this Court issued an Order requesting more information regarding some of the issues presented in Plaintiff's motion for expedited discovery. (R. Doc. 4). Specifically, this Court requested information as to which online pseudonyms the Doe defendants allegedly used, how the ISP addresses of the alleged Defendants were obtained since they are not automatically displayed on the P2P networks, what effects using an unsecured wireless network and or using a proxy would have on the reliability of these identified IP addresses, how CBC's software connected to and or accessed the files, and lastly, how CBC determines that a file was illegally downloaded. *Id.*

In response to this Order, Plaintiff responded that without further discovery, the potential Doe defendants are "only [identifiable] by the IP address of the internet connection they used to distribute Plaintiff's work without permission," as "no online pseudonyms" connecting the IP addresses to the illegally downloaded files were found. (R. Doc. 10, p. 1-2).

As to how the IP addresses are discovered, Plaintiff states that in a BitTorrent data transfer, "trackers [which are similar to large telephone directories] and users" manage the "exchange of IP address information between users." *Id.* at 3. Users may interrogate "trackers to search for other users," and may seek other users if they know of suitable individual that are participating in the distribution of a particular data set." *Id.* Plaintiff also stated that the IP addresses were discovered by CBC allegedly mimicking the "actions of a user within a BitTorrent network, to . . . interrogate trackers and request information from other users . . . including IP addresses. *Id.* at 3. Then, the monitoring software relies on "such IP addresses to gather lists of potential users distributing Plaintiff's content." *Id.* The last step involves CBC interrogating those lists to find "those willing to distribute Plaintiff's movie and engage in data transfer with those responsible by acquiring a part of Plaintiff's movie." *Id.*

Plaintiff further stated that unsecured wireless network does not affect the reliability of the monitoring software, as it is able to "identify the correct internet connection used to conduct the alleged copyright infringement." *Id.* at 4. However, Plaintiff argues that without further discovery, it is unable to determine whether or not the wireless network used was unsecured. *Id.* at 5. In any event, Plaintiff cites to *Malibu Media, LLC v. John Does 1, 6, 13, 14, and Bryan White*, 2:12-cv-1278 (E.D. Pa. June 11, 2013) for the proposition that the even if the network is unsecured, "the infringer is likely to be either the subscriber of the Internet connection or someone who resides within the same household." *Id.* at 4-5.

Plaintiff also states that using a proxy, a service that an Internet subscriber may purchase to hide his or her IP address, places an additional step in the discovery process, as a subscriber replaces his or her own IP address with the proxy server's IP address when communicating with remote

computers, therefore Plaintiff would need to make inquiries with the proxy server owner to determine the identity of the owner. (R. Doc. 5, p. 6)

Plaintiff further alleges that in order for successful data transfer to take place on BitTorrent networks, a sender and a recipient's IP address must be known both to the sender and to the recipient of data. *Id.* CBC's monitoring technology is able to identify the IP address of the proxy server, and successfully mimic a recipient and an acceptor of data transfers, just as the accused Doe Defendants involved in distributing Plaintiff's content on the BitTorrent. *Id.* Plaintiff contends that CBC's BitTorrent client functions similarly to other BitTorrents, but has one main difference; it is modified in a way that prevents it from distributing content. *Id.* at 6-7. Therefore, CBC is still able to download a part of the file that "resides on the source computer" and analyze it to determine that it is in fact the Plaintiff's movie. *Id.* at 7-8.

Due to CBC's ability to discover potential infringers based on their IP address, the Plaintiff's have filed suit against the potential Doe Defendants for alleged copyright infringement. As to the instant motion, Plaintiff's seek an order from this Court permitting it to issue Rule 45 subpoenas to various internet service providers ("ISP") to determine the identities of several unidentifiable Doe defendants, who potentially infringed on their copyright. (R. Doc. 3, p. 5-6).

## II. Standard of Review

Federal Rules of Civil Procedure ("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), except ... when authorized . . . by court order." *St. Louis Group, Inc., v. Metals and Additives Corp., Inc., et*

*al.*, 275 F.R.D. 236, 239 (S.D. Tex. 2011).[2] Although the Rules do not provide a standard for the court to use in exercising its authority to order expedited discovery, it is generally accepted that courts use one of the following two standards to determine whether a party is entitled to conduct such discovery: (1) the preliminary-injunction-style analysis set out in *Notaro v. Koch*, 95 F.R.D. 403 (S.D.N.Y.1982); or (2) the "good cause" standard, which has been used interchangeably with the "reasonableness" standard. *See St. Louis Group,* 275 F.R.D. at 239.

The Fifth Circuit has yet to adopt a standard, however, several district courts within the Fifth Circuit have expressly utilized the "good cause"[3] standard when addressing this issue. *St. Louis*, at 275 F.R.D. at 239-40; (*quoting* 8A Charles Alan Wright, Arthur R. Miller, Mary Kay Kane, & Richard L. Marcus, Federal Practice and Procedure § 2046.1 (3d ed. 2010)) ("[w]ithout any binding authority to the contrary, and in light of the fact that a majority of courts have adopted the 'good cause' standard, this Court believes that a showing of good cause should be made to justify an order authorizing discovery prior to the Rule 26(f) conference").[4]

The good cause analysis determines whether "good cause" exists to allow for expedited

---

[2] *See Edgenet, Inc. v. Home Depot U.S.A., Inc.*, 259 F.R.D. 385, 386 (E.D.Wis.2009); (citing *Am LegalNet, Inc. v. Davis*, 673 F.Supp.2d 1063, 1067 n. 4 (C.D.Cal.2009) (citing cases); *see also Dimension Data N. Am., Inc. v. Netstar–1, Inc.*, 226 F.R.D. 528, 531–532 (E.D.N.C.2005); *see also* 6 James Wm. Moore et al., Moore's Federal Practice § 26.121 (2011).

[3] *See St. Louis Group,* "[A]n increasing majority of district courts have instead adopted a 'good cause' standard to determine whether to authorize expedited discovery." *See, e.g., Merrill Lynch, Pierce, Fenner, & Smith, Inc. v. O'Connor*, 194 F.R.D. 618, 624 (N.D.Ill.2000); *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 275 (N.D.Cal.2002); *Ayyash v. Bank Al–Madina*, 233 F.R.D. 325, 327 (S.D.N.Y.2005); *Dimension Data*, 226 F.R.D. at 530–532.

[4] *See El Pollo Loco, S.A. de C.V. v. El Pollo Loco, Inc.*, 344 F.Supp.2d 986, 991 (S.D.Tex. 2004); *Energy Prod. Corp.*, 2010 WL 3184232, at *3; *Paul v. Aviva Life and Annuity Co.*, 2009 WL 3815949, at *1 (N.D. Tex. Nov. 12, 2009); *Rodale, Inc. v. U.S. Preventive Med., Inc.*, 2008 WL 4682043, at *1 (E.D. Tex. Oct. 21, 2008); *U.S. Commodity Futures Trading Comm'n v. M25 Inv., Inc.*, 2009 WL 3740627, at *1 (N.D. Tex. Sept. 29, 2009); *Philip Morris USA, Inc. v. Tin's, Inc.*, 2003 WL 22331256, at *1 (M.D. La. Apr. 23, 2003).

discovery. The good cause analysis considers factors such as the "breadth of the discovery requests, the purpose for requesting expedited discovery, the burden on the defendants to comply with the requests and how far in advance of the typical discovery process the request was made." *St. Louis Group*, 275 F.R.D. at 240, n. 4; (*citing Sunflower Elec. Power Corp. v. Sebelius*, 2009 WL 77430, at *2 (D. Kan. Mar. 20, 2009)); (*quoting In re Fannie Mae Derivative Litigation*, 227 F.R.D. 142, 143 (D.D.C. 2005)).

"In a 'good cause' analysis, a court must examine the discovery request 'on the entirety of the record to date and the reasonableness of the request in light of all the surrounding circumstances'." *St. Louis*, at 239-40; *Ayyash*, 233 F.R.D. at 327 (quoting *Merrill Lynch*, 194 F.R.D. at 624) (emphasis in original). Although the factors used by Courts may vary, good cause typically exists where "the need for expedited discovery outweighs the prejudice to the responding party." *St. Louis*, at 239-40; (quoting *Energy Prod. Corp. v. Northfield Ins. Co.*, 2010 WL 3184232, at * 3 (E.D. La. Aug. 6, 2010)); *see e.g., West Coast Productions, Inc., v. Does 1-169*, 2013 WL 3793969, at *1 (D. N.J. July 19, 2013); (quoting *Am. Legalnet, Inc. v Davis*, 673 F. Supp. 2d 1063, 1066 (C.D. Cal. 2009); (*accord Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 275-76 (N.D. Cal. 2002). The burden of showing good cause is on "the party seeking the expedited discovery." *See Qwest Commc'ns Int'l, Inc. v. WorldQuest Networks, Inc.*, 213 F.R.D. 418, 419 (D. Colo. 2003). A party seeking expedited discovery must narrowly tailor their requests in scope to the necessary information they seek. *St. Louis*, at 240; *Semitool*, 208 F.R.D. at 277 (discovery requests held to be narrowly tailored where Defendants' representative is not subjected to a free-ranging deposition); *Dimension Data*, 226 F.R.D. at 532 (E.D.N.C. 2005) (considering that the discovery request was not narrowly tailored in denying plaintiffs' motion for expedited discovery); *see also Monsanto Co. v.*

*Woods*, 250 F.R.D. 411, 413 (E.D. Mo. 2008) (citing *Irish Lesbian & Gay Org. v. Giuliani*, 918 F.Supp. 728, 730–31 (S.D.N.Y. 1996)) ("[C]ourts generally deny motions for expedited discovery when the movant's discovery requests are overly broad.").

However, Courts in the Fifth Circuit have stated that "irrespective of the standard applied, '[e]xpedited discovery is not the norm'." *St. Louis*, at 204; quoting *Merrill Lynch*, at 623. In limited circumstances though, district courts have allowed expedited discovery "when there is some showing of irreparable harm that can be addressed by limited, expedited discovery." *Id.* at 204-205. *See e.g., JP Morgan Chase Bank, N.A. v. Reijtenbagh*, 615 F.Supp.2d 278, 282–83 (S.D.N.Y. 2009) (granting expedited discovery to plaintiffs to determine the location of missing art pledged as collateral for $50 million promissory note); *Ayyash*, 233 F.R.D. at 326–27 (allowing expedited discovery on third-parties to locate assets in the United States relating to foreign defendants who had the incentive to hide those assets); *Pod-Ners, LLC v. N. Feed & Bean of Lucerne Ltd. Liab. Co.*, 204 F.R.D. 675, 676 (D. Colo. 2002) (allowing limited discovery in infringement action where bean plant variety at issue is a commodity subject to sale and consumption and might not be available for inspection at a later date); *McMann v. Doe*, 460 F.Supp.2d 259, 265–66 (D. Mass. 2006) (allowing expedited discovery on basis that showing of irreparable harm had been made because plaintiff could receive no remedy without knowing defendant John Doe's true name).

Courts also look to whether evidence would be lost or destroyed with time and whether the proposed discovery is narrowly tailored. *Killer Joe Nevada, LLC v. Does 1-31*, 2013 WL 3270384, at *1 (S. D. Ohio June 26, 2013); quoting *Best v. Mobile Streams, Inc.*, 2012 WL 5996222, *1 (S.D. Ohio November 30, 2012), citing *Arista Records, LLC v. Does 1–9*, 2008 WL 2982265 (S.D. Ohio July 29, 2008); *see also Arista Records, LLC v. Does 1–15*, 2007 WL 5254326 (S.D. Ohio May 17,

2007).

## III. Analysis

### A. Good Cause

Although the Court agrees with Plaintiff's argument that Courts across the country routinely grant expedited discovery requests in copyright and or patent infringement cases, "good cause" still must be demonstrated. *See Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 6-7 (D.D.C. 2008); *Revlon Consumer Prod. Corp. v. Jennifer Leather Broadway, Inc.*, 858 F.Supp. 1268, 1269 (S.D.N.Y.1994)). Plaintiffs argue that it has satisfied the "good cause" test as it has shown "(1) alleged copyright infringement; (2) danger that the ISP will not preserve the information sought; (3) the narrow scope of the information sought; (4) the conclusion that expedited discovery would substantially contribute to moving the case forward."

Here, Plaintiff contends that good cause exists to warrant the issuance of Rule 45 subpoenas as it is "unable to identify the Doe defendants" by their IP address, the date and time of alleged infringement, and because Defendants allegedly used "online pseudonyms . . . and not their true names." (*See* R. Doc. 3, p. 5). However, there are some discrepancies in Plaintiff's representations to the Court.

Plaintiff initially represented to this Court that it had "online pseudonyms" of potential Doe Defendants in its motion for leave to take expedited discovery. However, when this Court ordered Plaintiff to produce or verify these pseudonyms, Plaintiff revealed that it had only obtained the IP addresses and not pseudonyms of the potential Doe defendants. (*See* R. Doc. 3, p. 5; Doc. 5, p. 1).

An IP address is a unique numerical label assigned to a computer device participating in a computer network that uses internet protocol for communication, and serves two principal functions:

host or network interface identification and location addressing. [5] Each computer "is assigned a unique address somewhat similar to a street address or telephone number." *Id.* Once an IP address is captured, there are several methods that can be used to trace the user, one of which is to determine who owns the network, which can be done by searching registration IP registration databases, which are available across the world. *Id.* Another method is to review domain registration information via the "WHOIS" databases. *Id. See* **www.whois.com.**

Here, Plaintiff contends that there is no other reasonable means for it to discover the identities of the potential Doe defendants without this Court granting its request to issue Rule 45 subpoenas. However, upon further review, the Court finds that Plaintiff's contention is in error, as there are other ways that Plaintiff may discover the identities of the Doe defendants without the issuance of Court ordered discovery. For example, as cited above, inputting the IP addresses into an online database such as "WHOIS.Com" or "http://www.ip2location.com/demo" revealed more than just the IP address of the potential Doe defendants. It also showed that several of the address that Plaintiff provided, were not located in the Eastern District of Louisiana, several provided identifying information of the IP address holder.[6]

Additionally, for those IP addresses listed within the Eastern District of Louisiana, the service providers listed an email and telephone number to report and inquire about IP addresses and

---

[5] *See* Russ Smith, Consumer.Net, *IP Address: Your Internet Identity*, March 29, 1997. *See also* http://www.ntia.doc.gov/legacy/ntiahome/privacy/files/smith.htm (last visited on September 26, 2013).

[6] *See* R. Doc. 3-2, p. 2. IP Addresses #1: 96.33.128.176; #2:72.204.185.177 - WhoIs.com provided several names, email addresses, and telephone numbers associated with this address; #6: 68.121.212.139 - located in San Francisco, California - and a name, address and telephone number of the IP holder is provided; #7 - 98.164.93.35 - not located in Eastern District of Louisiana; #9: 66.190.200.36 – not located in Eastern District, but telephone number and name associated with IP provided; #11: 68.11.122.228 – not located in Eastern District, but telephone number to contact provided; #18: 68.225.79.34 not located in Eastern District, but telephone number to contact provided; #19: 70.171.74.206 – not located in Eastern District, but telephone number to contact provided; #20: 72.200.32.77.

potential abuse, such as the kind Plaintiff alleges here.[7] Therefore, the Court finds that Plaintiff has not shown good cause for expedited discovery on the basis of identifying the Doe defendants.

Plaintiff also contends that good cause exists for expedited discovery based on the risk of it losing the IP addresses tracing them to the potential Doe defendants. *See* R. Doc. 3, p. 15. However, Plaintiff also represented to the court that it obtained the IP address from its monitoring service, CBC, which allegedly "creates evidence logs for each user and then stores all this information in a database." *See* R. Doc. 3, p. 11; R. Doc. 3-2, p. 2. Therefore, the Court finds that Plaintiff is not at risk of losing any data that may typically be lost due to routine erasing of IP addresses, as Plaintiff has obtained a copy of the data using alternate methods as described above.

Lastly, in its memorandum in support, as well as in its reply to this Court's Order requesting further information, Plaintiff cites to cases that pre-suppose the IP address comes from stand-alone or single family unit dwelling homes. However, Plaintiff does not consider the possibility that the IP addresses could be from a shared, commercial establishment, such as a school, library, university, or a private multi-used dwelling, which has a single IP address but multiple users that make it difficult to determine whether the IP address is from an end user.

In fact, one of the IP address's provided # 3: 137.30.254.11 is allegedly from the "University of New Orleans" ("UNO"). *See* R. Doc. 3-2, p. 2. UNO is a public, undergraduate university, with thousands of people on its campus daily. The information we obtained shows that the IP address associated with UNO is actually located in a Computer Research Building, which further complicated the discovery of the alleged infringer. Issuing a broad Rule 45 subpoena, as that

[7] *Id.* at n. 6, #4: 75.131.80.254; # 5: 68.112.212.139; #8: 66.190.200.36; #9: 98.136.201.85; #10: 68.114.121.251; # 12: 24.158.218.17; #13:75.65.141.100; #14: 71.12.245.55; #15: 98.164.90.32; #16: 75.131.80.79; #17: 66.97.60.18.

requested by Plaintiff, for the identity of the potential Doe defendant who allegedly infringed on its copyright, would create a significant burden on UNO as it may not be able to determine which student, employee, or person, was the one who used one of its many computers.

This exact issue has been used to support denials of expedited discovery requests in similar copyright infringement cases across the country. In *Third Degree Films, Inc. v. John Does 1–110,* Civ. A. No. 2:12–cv–5817 (D. N. J. Jan. 17, 2013) an expedited discovery request to issue Rule 45 subpoenas was denied where Plaintiff was only able to identify the Doe defendants by an IP address. The Court stated that granting "Plaintiff's motion has the potential to permit Plaintiff to obtain detailed personal information of innocent individuals. This could subject an innocent individual to unjustified burden." *Id. See also West Coast Productions, Inc., v. Does 1-169*, 2013 WL 3793969, at *3 (D. N. J. July 19, 2013).

For example, in some situations, the "IP subscriber and the John Doe defendant may not be the same individual. Indeed, the infringer might be someone other than the subscriber; for instance, someone in the subscriber's household, a visitor to the subscriber's home or even someone in the vicinity that gains access to the network." *Id. See VPR Internationale v. Does 1–1017,* No. 11–2068, 2011 WL 8179128 (C.D. Ill. Apr. 29, 2011). Therefore, as the Court found in *Third Degree,* this court finds that "the potential to ensnare numerous innocent internet users into litigation [by permitting Rule 45 subpoenas] places a burden on them that outweighs Plaintiff's need for discovery." *Id. See also Pac. Century Int'l Ltd. v. Does,* 2011 WL 5117424 (N.D. Cal. Oct. 27, 2011).

**B. Future Ramifications of Permitting Expedited Discovery**

Plaintiff contends that expedited discovery is typically granted across the country in copyright infringement cases. However, Plaintiff's instant request for expedited discovery does not consider the mass amount of improper joinder claims that arise from a Court's granting of expedited discovery for Doe defendants. *See reFX Audio Software, Inc., v. Does 1-97,* 2013 WL 3766571, at *1-3, (E.D. Mo. July 16, 2013) (where the Court denied Plaintiff's Motion to Compel the AT&T's compliance with Rule 45 subpoenas seeking the identity and personal identifying information potential Doe defendants for being improperly joined).[8]

Although Plaintiff's instant motion does not request the joinder of all potential "Doe defendants" this Court recognizes the problems created across other District Court's that granted similar infringement expedited discovery requests, and declines to create such turmoil in this case, when Plaintiff may be able to ascertain the identities of the potential Doe defendants with further internet and or telephone communication and research. In *REFX,* the District Court states that "district courts across the country are considering *sua sponte* the issue of whether Doe defendants are properly joined in this type of litigation." *Id. See e.g., Kill Joe Nevada, LLC v. Does 1–81,* 2013 WL 2355545, *1 (N.D. Ga. 2013) (The court initially granted plaintiff's motion for expedited discovery, but later vacated the order upon further review of the joinder issue.); *reFX Audio Software, Inc., v. Does 1–82,* 2013 WL 500478 (D. Colo. Feb 11, 2013) ("[T]he Court sua sponte finds that joinder of all the named Defendants was not proper and dismisses the claims against John Doe Defendants 2–82 without prejudice to refiling separate cases against each Defendant."); *Safety*

[8] *reFX Audio Software Inc. v. Does 1-97,* "District courts are split over whether defendants may be joined in a single action based on their participation in a BitTorrent Swarm." *Kill Joe Nevada, LLC v. Does 1–81,* 2013 WL 2355545, *6; *see Malibu Media, LLC v. Does 1–21,* 2013 WL 2458290, *6 (N.D. Ind. May 22, 2013) (finding joinder appropriate); *Digital Sins, Inc. v. John Does 1–245,* 2012 WL 1744838, *2 (S.D.N.Y. May 15, 2012) (finding joinder inappropriate). "This issue is so divided that judges within the same district have even issued contrary opinions; however, "the number of courts holding that swarm joinder is not appropriate is growing." *See Voltage Pictures, LLC v. Does 1–198,* 2013 WL 1900597, *2 (D.Or. May 4, 2013)

*Point Products, LLC, et al., v. Does 1–14, et al.*, 2013 WL 1367078, *1 (N.D. Ohio Apr.4, 2013) ("[T]his Court finds sua sponte that Plaintiffs improperly joined Defendants and thus severs the claims[.]"). "[I]t is not only appropriate, but prudent to address the issue of joinder before litigation of this type is permitted to proceed further." *Malibu Media, LLC v. Reynolds*, 2013 WL 870618, *12 (N.D. Ill. Mar. 7, 2013).

Although the court is mindful of Plaintiff's intention to protect its copyright, the Court is mindful of the innocent individuals brought into litigations such as this, and realizes the potential, realistic risk of "coercive settlements" and unfair tactics that this type of "Doe defendant" discovery may ultimately cause. Therefore, the Court finds that Plaintiff has failed to demonstrate good cause sufficient to warrant granting expedited discovery of the potential doe defendants.

## IV. Conclusion

Accordingly.

**IT IS ORDERED** that the Plaintiff's's **Motion for Leave to Take Discovery Prior to Rule 26(f) Conference (R. Doc. 3)** is hereby **DENIED**.

New Orleans, Louisiana, this 30th day of September 2013

**KAREN WELLS ROBY**
**UNITED STATES MAGISTRATE JUDGE**