

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

**K-BEECH, INC.,**

**Plaintiff,**

**v.**

**1:11-cv-2968-WSD**

**JOHN DOES 1-47,**

**Defendant.**

---

**OPINION AND ORDER**

This matter is before the Court on Plaintiff K-Beech, Inc.’s Motion for Leave to Serve Third Party Subpoenas Prior to a Rule 26(f) Conference [3].

**I. BACKGROUND**

This is an action for alleged copyright infringement. On or about April 22, 2011, Plaintiff applied to register the copyright for a motion picture entitled “Virgins 4” (the “Work”).<sup>1</sup> The application was submitted pursuant to the United States Copyright Act of 1976 (“Copyright Act”), 17 U.S.C. §§ 101 et seq. The application is pending.

Plaintiff brings this action under the Copyright Act §§ 106 and 501 against forty-seven (47) anonymous Defendants identified only by their internet protocol

---

<sup>1</sup> The Work is an extremely pornographic and salacious work depicting a wide variety of sexual conduct and bodily functions.

(“IP”) addresses.<sup>2</sup> (Compl. ¶¶ 2, 4, 7.) Plaintiff alleges that each Defendant infringed on its copyright in the Work by sharing it on the BitTorrent internet peer-to-peer file sharing protocol. (Id. ¶¶ 13-42.) The alleged violations span four months, with the first violation occurring on April 16, 2011 and the last on July 16, 2011. (Ex. A to Compl.) All the violations are alleged to have occurred within the Northern District of Georgia. (Id.)

To determine the true identity of each Defendant from the subscriber information for each IP address, Plaintiff seeks, pursuant to Rule 45, to issue subpoenas to Comcast Cable (“Comcast”), an internet service provider (“ISP”).<sup>3</sup> (Mem. of Law in Supp. of Pl.’s Mot. for Leave to Serve Third Party Subpoenas at 4.) The subpoenas will specifically “demand the true name, address, telephone number, e-mail address and Media Access Control (‘MAC’) address of the Defendant to whom [Comcast] issued an IP address.” (Id.) Plaintiff states it intends to use the identity information it obtains from Comcast only to prosecute the claims in this action. (Id.) Without obtaining the information as to each Doe’s

---

<sup>2</sup> “An IP address is a number that is assigned by an Internet Service Provider (an ‘ISP’) to devices, such as computers, that are connected to the Internet.” (Compl. ¶ 8.)

<sup>3</sup> “The ISP to which each Defendant subscribes can correlate the Defendant’s IP address to the Defendant’s true identity.” (Id. ¶ 9.)

identity, Plaintiff cannot serve each Defendant and allow this action to proceed.

(Id. at 4-5.)

## II. DISCUSSION

### A. Misjoinder

The Court first considers whether the Defendants are properly joined under Rule 20 of the Federal Rules of Civil Procedure. Rule 20 provides that “[persons] . . . may be joined in one action as defendants if: (A) any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and (B) any question of law or fact common to all defendants will arise in the action.”

“The Court may issue orders – including an order for separate trials – to protect a party against embarrassment, delay, expense, or other prejudice . . . .” Fed. R. Civ.

P. 20(b). “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.

This case is part of an “outbreak of similar litigation . . . around the country,” in which copyright holders have attempted to assert claims against multiple unknown defendants by joining them, in often large numbers, into a single action. See On the Cheap, LLC v. Does 1-5011, No. C10–4472 BZ, 2011 WL

4018258, at \*1 (N.D. Cal. Sept. 6, 2011) (published order). The plaintiffs in these cases argue that when each defendant is one of many users simultaneously uploading and downloading a protected work, the defendant acts as part of a “swarm”<sup>4</sup> in a “series of transactions” involving a “common question of law or fact.” (See Compl. at 3). This practice is known as “swarm joinder,” and is the joinder theory relied upon by Plaintiff in this action.

---

<sup>4</sup> The BitTorrent swarm process has been described as follows:

In the BitTorrent vernacular, individual downloaders/distributors of a particular file are called “peers.” The group of peers involved in downloading/distributing a particular file is called a “swarm.” A server which stores a list of peers in a swarm is called a “tracker.” A computer program that implements the BitTorrent protocol is called a BitTorrent “client.”

The BitTorrent protocol operates as follows. First, a user locates a small “torrent” file. This file contains information about the files to be shared and about the tracker, the computer that coordinates the file distribution. Second, the user loads the torrent file into a BitTorrent client, which automatically attempts to connect to the tracker listed in the torrent file. Third, the tracker responds with a list of peers and the BitTorrent client connects to those peers to begin downloading data from and distributing data to the other peers in the swarm. When the download is complete, the BitTorrent client continues distributing data to the peers in the swarm until the user manually disconnects from the swarm or the BitTorrent client otherwise does the same.

Diabolic Video Prods., Inc. v. Does 1–2099, No. 10–CV–5865–PSG, 2011 WL 3100404, at \*1–2 (N.D. Cal. May 31, 2011); see also Camelot Distrib. Grp. v. Does 1 through 1210, No. 2:11-cv-02432 GEB KJN (E.D. Cal. Sept. 23, 2011).

The swarm joinder theory has been considered by various district courts, the majority of which have rejected it. See On the Cheap, 2011 WL 4018258, at \*1 (gathering cases) (published order). Downloading a work as part of a swarm does not constitute “acting in concert” with one another, particularly when the transactions happen over a long period. See, e.g., Hard Drive Productions, Inc. v. Does 1-188, No. C-11-01566 JCS, 2011 WL 3740473, at \*13 (N.D. Cal. Aug. 13, 2011) (“In fact, the nearly six-week span covering the activity associated with each of the addresses calls into question whether there was ever common activity linking the 51 addresses in this case.”).

Defendants alleged to have participated in “swarm” infringing often have different and divergent defenses<sup>5</sup> to the copyright violation claims and to allow them to be asserted in a single case would defeat, not enhance, judicial economy.<sup>6</sup>

---

<sup>5</sup> The variety of different defenses are often based on the circumstances of each defendant. Some may claim that the download did not occur, they were not involved in it, or their computer was incapable of the claimed conduct. The likelihood of different defenses demonstrates that each claim should be considered separately.

<sup>6</sup> The market value of a work like the one in this case is modest. The danger of swarm joinder is to enhance the proceeds from a Work by extracting settlement amounts that exceed the value of the Work and the litigation. It is conceivable that the swarm joinder device could encourage the creation of works not for their sales or artistic value, but to generate litigation and settlements. See On the Cheap, 2011 WL 4018258, at \*3 n.6. The risk of inappropriate settlement leverage is enhanced in a case like this involving salacious and graphic sexual content where a defendant

See CP Productions, Inc. v. Does 1-300, 2011 WL 737761 (N.D. Ill. Feb. 24, 2011)

(“No predicate has been shown for thus combining 300 separate actions on the cheap-if CP had sued the 300 claimed infringers separately for their discrete infringements, the filing fees alone would have aggregated \$105,000 rather than \$350.”)<sup>7</sup>

The facts here demonstrate why the swarm joinder pleading tactic is not appropriate in this action. The differing dates and times of each Defendant’s alleged sharing do not allow for an inference that the Defendants were acting in concert. While Defendants may have used the same peer-to-peer system, the Complaint does not allege they were sharing with each other. For example, Doe 1, who is alleged to have been in the swarm on June 30, 2011, is unlikely to have

---

may be urged to resolve a matter at an inflated value to avoid disclosure of the content the defendant was accessing.

<sup>7</sup> A limited number of courts have allowed swarm joinder for the narrow purpose of identifying anonymous defendants at the outset of the case. Courts adopting this view apply “the principle that permissive joinder seeks the broadest possible scope of action,” and reason that the nature of the BitTorrent protocol is that it inherently involves concerted action. See, e.g., Call of the Wild Movie, LLC v. Smith, 274 F.R.D. 334, 342 (D.D.C. 2011) (noting that “each additional user becomes a part of the network from where the file can be downloaded”). Based on the alleged dates of infringement, it is speculative, at best, that this principle applies here.

been in the swarm at the same time as Doe 2, who is alleged to have been in the swarm on May 24, 2011.<sup>8</sup>

The Court finds that Plaintiff has not adequately alleged that the Defendants were engaged in a common series of transactions as required by Rule 20, and joinder is not proper. In light of this and the variety of defenses likely to be raised, the Court further determines that joinder would not result in judicial economy and, thus, exercises its discretion to sever the claims against each Defendant. The Court dismisses John Does 2-47 without prejudice.

B. Protective Order

Rule 26(c)(1) permits the Court to issue, for good cause, “an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense.” Good cause encompasses not only “matters of delay and expense; discovery also may seriously implicate privacy interests of litigants and third parties.” Seattle Times Co. v. Rhinehart, 467 U.S. 20, 34-35 (1984). The discovery process gives litigants an opportunity to obtain “information that not only is irrelevant but if publicly released could be damaging to reputation and

---

<sup>8</sup> In light of the lack of proof of sharing with each other, it appears Defendants were joined as parties primarily because of their connection to this district. Plaintiff has filed at least two similar copyright actions, in the District of Colorado and the Eastern District of New York.

privacy . . . . [There is] a substantial interest in preventing this sort of abuse of [] processes.” Id. at 35.

In allowing Plaintiff to proceed against John Doe 1, the Court, in a case involving alleged copyright infringement of graphic pornographic material, is obligated to carefully manage and control discovery. BitTorrent mass copyright actions are now common. The potential for litigation abuse is real, and it is necessary to carefully control the discovery process.

In a similar case in California, after obtaining the information of the subscriber associated with an IP address implicated in alleged copyright infringement, the plaintiff returned to the court to ask for additional early discovery to inspect the “Subscriber's electronically stored information and tangible things, such as Subscriber's computer and the computers of those sharing his Internet network, for the purpose of finding the individual that unlawfully violated Plaintiff's copyrighted works.” Boy Racer, Inc. v. Does 1-52, 11-CV-2329-PSG (N.D. Cal. Sept. 13, 2011). The court observed that “every desktop, laptop, smartphone, and tablet in the subscriber's residence, and perhaps any residence of any neighbor, houseguest or other sharing his internet access, would be fair game.” Id. The need for reasonable management of the scope of discovery is self-evident.



In light of the allegations and content at issue in this case, the Court chooses to strictly manage the discovery requested. The Court will allow Plaintiff to issue a subpoena to Comcast to produce the true name, address, telephone number, e-mail address, and Media Access Control address for the IP address for John Doe 1 (the “Identity Information”) to outside counsel for the Plaintiff who have appeared in this case (the “Outside Lawyers”). The Outside Lawyers shall not disclose the Identity Information to any other person without the Court’s written approval. The Outside Lawyers may provide the Identity Information to the in-house counsel at Plaintiff who is responsible for this specific case. The Identity Information may be used solely in and only for the purposes of this action.<sup>9</sup>

Finally, if Plaintiff files actions in this district against John Does 2-47, or other John Doe defendants, alleging claims like those alleged in the Complaint filed in this action, Plaintiff shall designate such actions as “related” to this action against John Doe 1 and request they be assigned to this Court.

---

<sup>9</sup> These protections are imposed to protect the Defendant’s privacy interests. Cf. Steese, Evans & Frankel, P.C. v. S.E.C., No. 10-cv-01071-CMA-BNB, 2010 WL 5072011, at \*8-\*12 (D. Colo. Dec. 7, 2010) (ruling that disclosure, under the Freedom of Information Act, of information identifying an S.E.C. official who had downloaded pornography using a government computer without authorization, would constitute an unwarranted invasion of privacy and was not in the public interest).

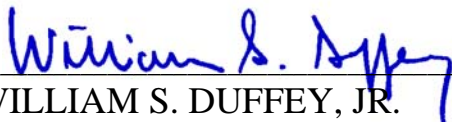
### III. CONCLUSION

For the foregoing reasons,

**IT IS HEREBY ORDERED** that John Does 2-47 are **SEVERED** and the claims against them are **DISMISSED WITHOUT PREJUDICE**.

**IT IS FURTHER ORDERED** that Plaintiff's Motion for Leave to Serve Third Party Subpoenas Prior to a Rule 26(f) Conference [3] is **GRANTED** under the restrictions set out in this order.

**SO ORDERED** this 29th day of September, 2011.

  
\_\_\_\_\_  
WILLIAM S. DUFFEY, JR.  
UNITED STATES DISTRICT JUDGE