

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF CONNECTICUT**

MALIBU MEDIA, LLC,

Plaintiff,

v.

JOHN DOE, subscriber assigned IP address  
32.210.216.224,

Defendant.

Civil Action No.  
3:18-cv-00355 (CSH)

April 9, 2019

**RULING ON PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY  
SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE**

**HAIGHT, Senior District Judge:**

Plaintiff Malibu Media LLC ("Plaintiff" or "Malibu Media") alleges that defendant John Doe ("Defendant" or "Defendant Doe"), identified only by his or her Internet Protocol ("IP") address, has unlawfully distributed four of Plaintiff's copyrighted adult films using BitTorrent, a peer-to-peer file sharing system. Doc. 1 at ¶ 11. Pursuant to Rule 26(d)(1) of the Federal Rules of Civil Procedure, Malibu Media moves for leave to serve a third-party subpoena on Defendant's internet service provider ("ISP"), Frontier Communications, prior to a Rule 26(f) Conference for the limited purpose of discovering Defendant's identity so that Plaintiff may effectuate service and proceed in litigating this case. Doc. 7. For the reasons set forth below, the Court finds that there is good cause to grant the motion, as limited by the conditions delineated herein.

**I. DISCUSSION**

**A. Legal Standard**

In general, a party may not propound discovery in advance of a Rule 26(f) conference. Fed.

R. Civ. P. 26(f); *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 241 (S.D.N.Y. 2012) (in general parties "may not initiate discovery prior to satisfying the meet and confer requirement of Fed. R. Civ. P. 26(f)"). However, courts may authorize earlier discovery if they determine it is warranted applying a "flexible standard of reasonableness and good cause." *Artista Records, LLC v. Doe*, 604 F.3d 110, 115 (2d Cir. 2010); *see also Malibu Media, LLC v. John Doe Subscriber Assigned IP Address 173.68.5.86*, No. 1:16-CV-02462(AJN), 2016 WL 2894919, at \*2 (S.D.N.Y. May 16, 2016) (collecting cases). In evaluating subpoenas seeking identifying information from ISPs regarding alleged copyright infringers, courts examine the following factors:

(1) the concreteness of the plaintiff's showing of a prima facie claim of actionable harm, (2) the specificity of the discovery request, (3) the absence of alternative means to obtain the subpoenaed information, (4) the need for the subpoenaed information to advance the claim, and (5) the objecting party's expectation of privacy.

*Arista Records, LLC*, 604 F.3d at 119 (quoting *Sony Music Entm't, Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 564-65 (S.D.N.Y. 2004)). If "[a]pplication of these 'principal factors' confirms that the Plaintiff is entitled" to the requested subpoena, the motion for early discovery will be granted for good cause. *Malibu Media*, 2016 WL 2894919, at \*2 (quotation marks and citation omitted).

## **B. Application**

First, Plaintiff has stated a prima facie claim for copyright infringement. To state a prima facie claim for infringement, Plaintiff must plausibly allege (1) ownership of a valid copyright and (2) unauthorized copying of original elements of the copyrighted work. *See Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 361 (1991). When infringement allegations arise from peer-to-peer file sharing, a plaintiff makes "a concrete, prima facie case of copyright infringement by alleging ownership of the registered copyright and alleging unlawful downloading, copying, and

distribution of this work by specifying the type of technology used, the IP address from which the file was accessed and shared, and the date and time of the infringement." *Strike 3 Holdings, LLC v. John Doe*, No. 3:18-CV-1332 (CSH), 2018 WL 4846676, at \*2 (D. Conn. Oct. 5, 2018) (internal quotation marks and citation omitted); *see also Sony Music*, 326 F. Supp. 2d at 565-66 ("[T]he use of P2P [peer-to-peer] systems to download and distribute copyrighted music has been held to constitute copyright infringement." (collecting cases)); *Patrick Collins, Inc. v. John Doe I*, 945 F. Supp. 2d 367, 375 (E.D.N.Y. 2013) ("Indeed, every court to have addressed this issue has found a sufficiently alleged copyright infringement claim based on BitTorrent technology, even when the defendant was merely identified with an IP address.").

Malibu Media has alleged that it owns copyrights in the adult films at issue. *See* Doc. 1 ¶ 30. Malibu Media has also made a plausible showing that wrongful "copying" of that work occurred by alleging that its investigator, IPP International UG, established a direct connection with the Defendant's IP address and downloaded the copyrighted films at issue from the Defendant using BitTorrent. *Id.* ¶¶ 18-20; *see also* Doc. 1-1 and 1-2 (Ex. A & B, respectively). Under these facts, Plaintiff has stated a prima facie case for actionable harm due to copyright infringement.

*Second*, in order to show "good cause" for early discovery, Plaintiff must narrowly tailor and specifically identify the information sought by the discovery request. Here, the subpoena is limited and seeks only "concrete and narrow information: the name and address of the subscriber associated with [Defendant's] IP address." *John Wiley & Sons, Inc. v. Doe Nos. 1-30*, 284 F.R.D. 185, 190 (S.D.N.Y. 2012); *see also Malibu Media*, 2016 WL 4574677, at \*6 (subscriber's identity and address constitute "highly specific" information). This request is sufficiently specific and narrowly tailored because it seeks only the information necessary to enable Plaintiff to effectuate service on the

Defendant. The procedural safeguards set forth in Section I(C), *supra*, will further ensure that the scope of discovery is no broader than necessary. Accordingly, the second factor weighs in favor of granting leave to serve the subpoena.

*Third*, there must be no "alternative means to obtain the subpoenaed information." *Arista Records*, 604 F.3d at 119 (citation omitted). In the present case, Plaintiff "knows Defendant only by his or her IP address." Doc. 7-1 at 10. With no other identifying information about Defendant, the only way that Plaintiff can obtain the information that it seeks—Defendant's true name and address—is through a subpoena of the ISP. *See id.* at 10-13 ("The government, law enforcement officials, criminal and civil judges, and ISPs alike all acknowledge that subpoenaing an ISP is the only way to identify an internet subscriber."); *see also Malibu Media, LLC v. Doe*, No. 1:15-cv-01834, 2015 WL 4403407, \*2 (S.D.N.Y. July 20, 2015) (denying motion to quash and explaining that "subpoenaing the ISP . . . is the *only* means to obtain identifying information"). Indeed, Plaintiff attempted to ascertain Defendant's identity in other ways prior to submitting its motion, including through use of web search tools and consultation with a computer forensics investigator, to no avail: the information is in the exclusive control of the ISP. Doc. 7-1 at 12-13. Plaintiff has therefore established that it lacks alternative means to obtain the information at issue.

*Fourth*, Plaintiff must show that the subpoenaed information is necessary to advance the claim at issue. As stated *supra*, litigation cannot proceed without the subpoenaed information, which is necessary to serve process on the Defendant. *See Sony Music*, 326 F. Supp. 2d at 566 ("Ascertaining the identities and residences of the Doe defendants is critical to plaintiffs' ability to pursue litigation, for without this information, plaintiffs will be unable to serve process."); *Arista Records LLC v. Does 1-4*, 589 F. Supp. 2d 151, 153 (D. Conn. 2008) ("Because learning the true

identities of the pseudonymous individuals alleged to have violated Plaintiffs' copyrights is essential to their prosecution of this litigation, Plaintiffs have demonstrated their need for expedited discovery."); *Malibu Media, LLC v. Doe*, No. 15-CV-3504 (JFB) (SIL), 2016 WL 4444799, at \*11 (E.D.N.Y. Aug. 23, 2016) ("Without learning the Defendant's identity and address, the Plaintiff will be unable to serve process and pursue its claim." (citation omitted)). This factor, too, weighs heavily in favor of granting leave to serve the subpoena.

*Fifth*, the Court weighs the Defendant's right to privacy against the Plaintiff's interest in obtaining the information. Plaintiff has a strong, legitimate interest in protecting its copyrighted material from unauthorized distribution. Defendant, on the other hand, has no legitimate expectation of privacy in identifying information that has already been exposed to a third party, the internet service provider. *See United States v. Ulbricht*, 858 F.3d 71, 96-97 (2d Cir. 2017) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," including "IP address information and similar routing data, which reveal the existence of connections between communications devices without disclosing the content of the communications." (quoting *Smith v. Maryland*, 442 U.S. 735 (1979))); *see also, e.g., Sony Music*, 326 F. Supp. 2d at 566 ("[D]efendants have little expectation of privacy in downloading and distributing copyrighted songs without permission."); *Raw Films, Ltd. v. John Does 1-15*, No. CIV.A. 11-7248, 2012 WL 1019067, at \*8 (E.D. Pa. Mar. 26, 2012) (The "expectation of internet users engaging in online file-sharing . . . is at most minimal because those individuals have already voluntarily given up certain information by engaging in that behavior."). Indeed, in cases in which parties have argued that the First Amendment protected their anonymous speech in using their IP addresses, the Second Circuit has held that copyright infringers are not entitled to shield their

identities from those who seek to enforce their claims under copyright law. *See Sony Music*, 326 F. Supp. 2d at 567 ("[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."); *Artista Records*, 604 F.3d at 118 (rejecting defendant's motion to quash subpoena of an ISP on First Amendment grounds because "to the extent that anonymity is used to mask copyright infringement or to facilitate such infringement by other persons, it is unprotected by the First Amendment."); *Strike 3*, 2017 WL 5001474, at \*5, n.1 (permitting plaintiff to subpoena ISP and holding that "[t]he First Amendment does not protect copyright infringement."); *see also Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 451 (C.D. Cal. 2007) ("To the extent the [internet] users are engaged in copyright infringement, the First Amendment affords them no protection whatsoever." (citing *Harper & Row Publishers, Inc. v. Nation Enters*, 471 U.S. 539, 559 (1985))). District courts within this Circuit have thus consistently permitted copyright plaintiffs to obtain infringers' identifying information based on their IP addresses. *See, e.g., Arista Records, LLC*, 604 F.3d at 124 (holding defendant's "expectation of privacy for sharing copyrighted [works] through an online file-sharing network [was] simply insufficient to permit him to avoid having to defend against a claim of copyright infringement"); *Rotten Records, Inc. v. Doe*, 108 F. Supp. 3d 132, 134 (W.D.N.Y. 2015) ("Plaintiff's interest in learning Defendant's name and address outweighs Defendant's privacy interest." (citing *Arista Records*, 604 F.3d at 124)). Accordingly, the Court finds that the Doe Defendant's right to remain anonymous must give way to Plaintiff's right to use the judicial process to pursue its allegedly meritorious copyright infringement claim. Moreover, the Doe Defendant lacks the right under the Fourth Amendment to protect his IP address from revelation where he has voluntarily shared such information with his ISP.

In sum, taken together, the elements set forth in *Artista* weigh strongly in favor of permitting Plaintiff to take limited early discovery in order to determine the identity of Defendant Doe.

**C. Conditions and Limitations**

Although Plaintiff will be permitted to take limited early discovery, the Court recognizes and shares the concern—expressed by many other courts around the nation—that the nature of the films allegedly distributed in this action may make Defendant liable to accept an otherwise unwelcome settlement in order to prevent disclosure of Defendant's identifying information. *See, e.g., Malibu Media, LLC v. John Does 1–5*, 285 F.R.D. 273, 278 (S.D.N.Y. 2012) ("[T]here is a fear that regardless of a defendant's actual culpability, [the Defendant] may feel compelled to settle the lawsuit confidentially in order to avoid the embarrassment of being named as a defendant in a case about the alleged illegal trading of a pornographic film." (internal quotation marks omitted)); *Malibu Media, LLC v. Doe*, No. 15-CV-4381(JFK), 2015 WL 4923114, at \*1 (S.D.N.Y. Aug. 18, 2015) ("[C]ourts in this district have expressed concern . . . that disclosure of a defendant's name or other identifying information in cases involving infringement of adult films could lead to abusive litigation through coercion."); *Malibu Media, LLC v. Doe*, No. 15- CV-4369 (AKH), 2015 WL 4092417, at \*2 (S.D.N.Y. July 6, 2015) (noting that "the late Judge Harold Baer, Jr. explained that [i]n such cases, there is a risk not only of public embarrassment for the misidentified defendant, but also that the innocent defendant may be coerced into an unjust settlement with the plaintiff to prevent the dissemination of publicity surrounding unfounded allegations." (quotation marks and citation omitted)).

In light of these concerns, the Court sets forth the following conditions and limitations:

1. Plaintiff may subpoena Defendant's ISP *only to obtain Defendant's name and*

*address*, but not Defendant's e-mail addresses or telephone numbers. As set forth above, Plaintiff may only use this information (name and address) for the purposes of this litigation. Plaintiff is ordered not to disclose Defendant's name or address, or any other identifying information other than Defendant's IP number, that Plaintiff may subsequently learn. Plaintiff shall not threaten to disclose any of Defendant's identifying information. Defendant will be permitted to litigate this case anonymously unless and until this Court orders otherwise and only after Defendant has had an opportunity to challenge the disclosure. **Therefore, Plaintiff is ordered not to publicly file any of Defendant's identifying information and to file all documents containing Defendant's identifying information under seal.**

2. As to timing, Plaintiff may immediately serve a Rule 45 subpoena on Defendant's ISP to obtain Defendant's name and current and permanent address. Plaintiff is reminded that it must serve Defendant with a copy of the Complaint, this Ruling, and the subpoena.
3. After having been served with the subpoena, the ISP will delay producing to Plaintiff the subpoenaed information until after it has provided Defendant Doe with:
  - a. notice that this suit has been filed naming Defendant as the one who allegedly downloaded copyright protected work;
  - b. a copy of the subpoena, the Complaint filed in this lawsuit, and this Ruling; and
  - c. notice that the ISP will comply with the subpoena and produce to Plaintiff the information sought in the subpoena unless, within sixty (60) days of service



of the subpoena on Defendant by the ISP, Defendant files a motion to quash the subpoena or for other appropriate relief in this Court. If a timely motion to quash is filed, the ISP shall not produce the subpoenaed information until the Court acts on the motion.

4. Defendant's ISP will have sixty (60) days from the date of service of the Rule 45 subpoena upon it to serve Defendant Doe with a copy of the Complaint, this Ruling, and the subpoena. The ISP may serve Defendant Doe using any reasonable means, including written notice sent to his or her last known address, transmitted either by first class mail or via overnight service.
5. Defendant Doe shall thereafter have sixty (60) days from the date of service of the Rule 45 subpoena and this Ruling upon him or her to file any motions with this Court to contest the subpoena (including a motion to quash or modify the subpoena), as well as to request to litigate the subpoena anonymously. During this sixty (60) day period, if Defendant contests the subpoena, he or she shall notify the ISP, which shall then not turn over the Defendant's identifying information to Plaintiff. Upon expiration of the sixty (60) days, if Defendant has filed a motion to quash or modify the subpoena, or a request to litigate the subpoena anonymously, the ISP may not turn over any information to Plaintiff unless and until the Court resolves the issue(s) and instructs the ISP when it may, if ever, turn the requested discovery over to the Plaintiff. In the meantime, the ISP must preserve all subpoenaed information pending the resolution of any timely filed motion to quash.
6. Alternatively, if the sixty (60) day period referenced in the preceding paragraph

lapses without Defendant or the ISP contesting the subpoena, the ISP shall have fourteen (14) days thereafter to produce the information which is responsive to the subpoena to the Plaintiff.

7. Defendant's ISP shall confer with Plaintiff and shall not assess any charge in advance of providing the information requested in the subpoena. If Defendant's ISP receives a subpoena and elects to charge for the costs of production, it shall provide a billing summary and cost report to Plaintiff.
8. Plaintiff may not solicit settlement of this case prior to service of the Complaint upon the Defendant. Plaintiff has consented to this condition with the understanding that defendants in such infringement cases may feel coerced to settle to avoid a risk of public embarrassment.

### **III. CONCLUSION**

For the foregoing reasons, the Court GRANTS the Plaintiff's Motion for Leave to Serve a Third Party Subpoena Prior to a Rule 26(f) Conference [Doc. 7], subject to the conditions and limitations set forth in Section I (C) of this Ruling, and ORDERS, as follows:

1. Under relevant Second Circuit authority, Plaintiff Malibu Media has established that "good cause" exists for the Court to grant Plaintiff leave to serve a third party subpoena on the ISP, Frontier Communications, for the purpose of determining the identity of the alleged infringer, Defendant Doe.
2. Plaintiff may serve the ISP with a Rule 45 subpoena commanding the ISP to provide Plaintiff with the true name and address of the Defendant to whom the ISP assigned the indicated IP address, as set forth in Exhibit A to the Complaint. Plaintiff shall

attach to any such subpoena a copy of this Ruling.

3. Plaintiff may also serve a Rule 45 subpoena in the same manner as described in the preceding paragraph on any service provider who, in response to a subpoena, is identified as a provider of Internet services to the Defendant.
4. If the ISP or another service provider (as described in ¶ 3, *supra*) qualifies as a "cable operator," as defined by 47 U.S.C. § 522(5), it shall comply with 47 U.S.C. § 551(c)(2)(B) by sending a copy of this Ruling to the Defendant.<sup>1</sup> Section 551(c)(2)(B) states in relevant part:

A cable operator may disclose such [personally identifying] information if the disclosure is . . . made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed.

5. Plaintiff may only use the information disclosed in response to a Rule 45 subpoena served on the ISP for the purpose of protecting and enforcing Plaintiff's rights, as set forth in its Complaint [Doc. 1].

It is **SO ORDERED**.

Dated: New Haven, Connecticut  
April 9, 2019

/s/ Charles S. Haight, Jr.  
CHARLES S. HAIGHT, JR.  
Senior United States District Judge

---

<sup>1</sup> 47 U.S.C. § 522(5) defines the term "cable operator" as "any person or group of persons (A) who provides cable service over a cable system and directly or through one or more affiliates owns a significant interest in such cable system, or (B) who otherwise controls or is responsible for, through any arrangement, the management and operation of such a cable system."