

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**UNITED STATES DISTRICT COURT**  
EASTERN DISTRICT OF CALIFORNIA

MALIBU MEDIA, LLC,  
Plaintiff,

Case No. 1:15-cv-01950-AWI-SKO

v.

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

JOHN DOE, subscriber assigned IP address  
172.9.210.109,  
Defendant.

---

**I. INTRODUCTION**

Plaintiff Malibu Media, LLC ("Plaintiff") filed a complaint against John Doe ("Defendant") on December 30, 2015, alleging infringement claims pursuant to the United States Copyright Act of 1976. Plaintiff claims Defendant is a persistent online infringer of Plaintiff's copyrighted films. On March 1, 2016, Plaintiff filed a motion for leave to serve a third-party subpoena prior to a Rule 26(f) conference. (Doc. 6.) As Defendant has not yet been identified by name, no opposition was filed. Pursuant to Local Rule 230(g), the Court finds Plaintiff's motion suitable for decision without oral argument, and no hearing on this matter shall be set. For the reasons discussed below, Plaintiff's motion is GRANTED subject to the noted restrictions herein.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

## II. BACKGROUND

Plaintiff is a limited liability company that produces copyrighted adult films. Defendant is alleged to have used the BitTorrent file distribution network to download adult pornographic films subject to copyrights held by Plaintiff. Defendant has been identified in this lawsuit only by an Internet Protocol address ("IP Address") assigned to a customer on a specific date by an Internet Service Provider ("ISP") and through which the copyrighted works were allegedly downloaded.

BitTorrent technology has been described by several courts, including the district court in *Malibu Media, LLC v. Doe*, No. 15-cv-4369 (AKH), 2015 WL 4092417, \*1-2 (S.D.N.Y. July 6, 2015):

BitTorrent is a peer-to-peer file-sharing protocol that allows users to transfer large files over the internet by breaking the complete file (the "Seed") into small pieces to be downloaded in parts. Other users ("Peers") downloaded a small "torrent" file that contains an index of the pieces and directions for connecting to the Seed. When Peers connect to the Seed, they download pieces of the file at random, and begin sharing each piece once it has completed downloading. After all the pieces are downloaded, the BitTorrent software reassembles the pieces into a complete file for the Peer to view.

BitTorrent is distinguishable from other file sharing protocols by its users' ability to upload and download files simultaneously. This non-sequential download structure reduces the bottleneck of traffic, which allows for faster download speeds. The Peers that are uploading and downloading the same Seed file from each other at a given point in time are collectively called a "Swarm." Members of a Swarm are able to see the IP addresses of other Peers to whom they are connected. In addition, BitTorrent "tracks" the pieces of a file as it is shared, so Peers can identify the IP addresses from which the file was downloaded.

*Id.* (citing *Patrick Collins, Inc. v. Doe 1*, 288 F.R.D. 233 (E.D.N.Y. 2012), *Next Phase Distribution, Inc. v. John Does 1-27*, 284 F.R.D. 165 (S.D.N.Y. 2012), *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80 (E.D.N.Y. 2012)).

Plaintiff has filed a motion for leave to serve a third-party subpoena prior to a Federal Rule of Civil Procedure 26(f) discovery conference, requesting permission to initiate discovery to identify the account subscriber associated with the IP Address used to download Plaintiff's copyrighted films, notwithstanding the provision of Rule 26(d)(1) which precludes a party from seeking discovery from any source before the parties have conferred as required by Rule 26(f).

1 Plaintiff contends a Rule 45 subpoena to the ISP must be permitted to obtain the identity of the  
2 customer assigned the IP Address on the dates<sup>1</sup> in question to ascertain the identity of the person  
3 responsible for unauthorized downloading of the copyrighted works produced by Plaintiff.  
4 Plaintiff maintains there is no other way for it to obtain this information.

### 5 **III. DISCUSSION**

#### 6 **A. Legal Standard**

7 Generally, a party may not conduct discovery before the parties have met and conferred  
8 pursuant to Federal Rule of Civil Procedure 26(f) "except in a proceeding exempted from initial  
9 disclosure under Rule 26(a)(1)(B), or when authorized by these rules, by stipulation, or by court  
10 order." Fed. R. Civ. P. 26(d)(1). The Ninth Circuit has held that when a defendant's identity is  
11 unknown at the time the complaint is filed, a court may grant the plaintiff leave to take early  
12 discovery to determine the defendant's identity "unless it is clear that discovery would not uncover  
13 the identit[y], or that the complaint would be dismissed on other grounds." *Gillespie v. Civiletti*,  
14 629 F.2d 637, 642 (9th Cir. 1980). District courts in the Ninth Circuit have permitted expedited  
15 discovery prior to the Rule 26(f) conference upon a showing of "good cause." *See, e.g., In re*  
16 *Countrywide Fin. Corp. Derivative Litig.*, 542 F. Supp. 2d 1160, 1179 (C.D. Cal. 2008) (citing  
17 *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273 (N.D. Cal. 2002)). "Good cause exists  
18 where the need for expedited discovery, in consideration of the administration of justice,  
19 outweighs the prejudice to the responding party." *In re Countrywide Fin. Corp. Derivative Litig.*,  
20 542 F. Supp. 2d at 1179 (citation and quotation marks omitted).

#### 21 **B. Plaintiff Has Established Good Cause to Serve a Third-Party Subpoena**

22 District courts within the Ninth Circuit have typically found good cause supporting early or  
23 expedited discovery in cases where the plaintiff alleged copyright infringement accomplished  
24 through distribution of the work over a peer-to-peer network, and where the plaintiff sought early  
25 discovery to obtain the identities and contact information of the alleged infringers from associated  
26 ISPs. *See, e.g., Berlin Media Art E.K. v. Does 1 through 146*, No. S-11-2039 KJM GGH, 2011

---

27 <sup>1</sup> In its complaint, Plaintiff specifically identifies 137 separate times between July 2013 and October 2015 that  
28 Defendant downloaded, copied, and distributed a complete copy of Plaintiff's works without authorization. (Doc. 1-1,  
Exhibit A.)

1 WL 4056167, at \*2 (E.D. Cal. Sept. 12, 2011) (unpublished) (granting leave to serve Rule 45  
2 subpoena to identify doe defendant); *Malibu Media, LLC v. John Does 1-10*, No. 2:12-cv-3623-  
3 ODW (PJWx), 2012 WL 5382304 (C.D. Cal. June 27, 2012).

4 **1. Balancing Interests in the Context of Copyright Infringement**

5 In applying the good cause standard in cases where the unknown defendant is an  
6 anonymous internet user, courts give careful consideration to the diverging interests of both the  
7 party seeking the discovery and the unknown Doe defendant:

8 With the rise of the Internet has come the ability to commit certain tortious  
9 acts, such as defamation, copyright infringement, and trademark infringement,  
10 entirely on-line. The tortfeasor can act pseudonymously or anonymously and may  
11 give fictitious or incomplete identifying information. Parties who have been  
12 injured by these acts are likely to find themselves chasing the tortfeasor from  
13 Internet Service Provider (ISP) to ISP, with little or no hope of actually discovering  
14 the identity of the tortfeasor.

15 In such cases the traditional reluctance for permitting filings against John  
16 Doe defendants or fictitious names and the traditional enforcement of strict  
17 compliance with service requirements should be tempered by the need to provide  
18 injured parties with a[] forum in which they may seek redress for grievances.  
19 However, this need must be balanced against the legitimate and valuable right to  
20 participate in online forums anonymously or pseudonymously. People are  
21 permitted to interact pseudonymously and anonymously with each other so long as  
22 those acts are not in violation of the law. This ability to speak one's mind without  
23 the burden of the other party knowing all the facts about one's identity can foster  
24 open communication and robust debate. Furthermore, it permits persons to obtain  
25 information relevant to a sensitive or intimate condition without fear of  
26 embarrassment. People who have committed no wrong should be able to  
27 participate online without fear that someone who wishes to harass or embarrass  
28 them can file a frivolous lawsuit and thereby gain the power of the court's order to  
29 discover their identity.

30 *Columbia Ins. Co. v. seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999). As it pertains to  
31 copyright infringement cases involving the internet, many courts have documented growing  
32 concerns about "copyright trolls," "roughly defined as plaintiffs who are 'more focused on the  
33 business of litigation than on selling a product or service or licensing their [copyrights] to third  
34 parties to sell a product or service.'" *Malibu Media, LLC*, 2015 WL 4092417, at \* 2 (quoting  
35 Matthew Sag, *Copyright Trolling, An Empirical Study*, 100 Iowa L. Rev. 1105, 1108 (2015)).

1 "The paradigmatic troll plays a numbers game in which it targets hundreds or  
2 thousands of defendants, seeking quick settlements priced just low enough that it is  
3 less expensive for the defendant to pay the troll rather than defend the  
4 claim." [Matthew Sag, *Copyright Trolling, An Empirical Study*, 100 Iowa L. Rev.  
5 1105, 1108 (2015)]. The lawsuits most frequently target anonymous John Does for  
6 alleged infringement related to the use of BitTorrent. Indeed, of "the 3,817  
7 copyright law suits filed in 2013, over 43% were against John Does and more than  
8 three-quarters of those related to pornography." *Id.* at 1108–09. But almost none  
9 ever reaches a hearing. Rather, the "lawsuits are filed to take advantage of court  
10 ordered discovery [under Fed. R. Civ. P. 26(d)] to break the veil of anonymity that  
11 separates IP addresses from the account information of actual human  
12 beings." *Id.* at 1109; *see also Digital Sin, Inc. v. Does 1–176*, 279 F.R.D. 239, 241  
(S.D.N.Y.2012). They then use this information to quickly negotiate settlements  
on mass scale without any intention of taking the case to trial. [footnote omitted]  
*See, e.g., Media Prods., Inc., DBA Devil's Film v. John Does 1–26*, No. 12–cv–  
3719, at 4 (S.D.N.Y. June 18, 2012) (explaining that the settlements in these  
BitTorrent cases are "are for notoriously low amounts relative to the possible  
statutory damages, but high relative to the low value of the work and minimal costs  
of mass litigation. Cases are almost never prosecuted beyond sending demand  
letters and threatening phone calls.").

13 *Malibu Media, LLC*, 2015 WL 4092417, at \* 2.

14 The danger of copyright trolls is particularly acute in the context of pornography. In these  
15 cases, "there is a risk not only of public embarrassment for the misidentified defendant, but also  
16 that the innocent defendant may be coerced into an unjust settlement with the plaintiff to prevent  
17 the dissemination of publicity surrounding unfounded allegations." *Media Prods., Inc.*, No. 12-cv-  
18 3719, at 4; *see also Malibu Media, LLC v. Does 1-5*, No. 12-cv-2950 (JPO), 2012 WL 2001968, at  
19 \*1 (S.D.N.Y. June 1, 2012) ("This Court shares the growing concern about unscrupulous tactics  
20 used by certain plaintiffs, especially in the adult film industry, to shake down the owners of  
21 specific IP addresses from which copyrighted adult films were allegedly downloaded.").

22 The abuses of Malibu Media in particular have been discussed by a court in the Southern  
23 District of New York:

24 However, Malibu's corporate strategy relies on aggressively suing for  
25 infringement and obtaining accelerated discovery of the IP address holder's identity  
26 from the ISP. It then seeks quick, out-of-court settlements which, because they are  
27 hidden, raise serious questions about misuse of court procedure. Judges regularly  
28 complain about Malibu. For example, in May, Judge Timothy Black of the  
Southern District of Ohio surveyed some of Malibu's questionable conduct in  
litigations across the country. See Order to Show Cause, ECF Doc. No. 15, *Malibu  
Media, LLC v. Ryan Ramsey*, No. 14–cv–718 (S.D. Ohio May 26, 2015). He found

1 that, while "Malibu Media asserts that it is necessary to invoke the Court's  
2 subpoena power to 'propound discovery in advance of a Rule 26(f) conference' . . .  
3 [,] not a single one of these 60 cases [filed in this district over the previous 12  
4 months] has even progressed to a Rule 26(f) conference." *Id.* at 5. Indeed, most  
5 are dismissed even without the issuance of a summons. *Id.* Malibu's motive is to  
6 use the federal courts only to obtain identifying information in order to coerce fast  
7 settlements. *Id.* at 8 (citing *Malibu Media, LLC v. Does 1-54*, No. 12-cv-1407,  
8 2012 WL 303[03]02, at \*5 (D. Colo. July 25, 2012); *Malibu Media, LLC v. Does*,  
9 923 F. Supp. 2d 1339, 1345-46 (M.D.Fla.2013)).

10 Malibu effectuates its strategy by employing tactics clearly calculated to  
11 embarrass defendants. For example, in recent complaints filed in the Wisconsin  
12 federal courts, an attached "Exhibit C" listed additional pornographic videos  
13 downloaded to the defendants' IP addresses using BitTorrent. The titles in Exhibit  
14 C were extremely racy and lewd, and the district court sanctioned Malibu when it  
15 learned that Malibu did not even own the copyrights for the titles; rather, it had  
16 gratuitously listed them to coerce larger, faster settlements by further shaming  
17 defendants. *See Malibu Media LLC v. John Doe* subscriber assigned IP address  
18 24.183.51.58, 2013 WL 4821911 (W.D. Wis. Sep. 10, 2013); *Malibu Media, LLC*  
19 *v. Doe*, No. 13-cv-536, 2013 WL 6579338, at \*4 (E.D. Wis. Dec. 12, 2013).

20 When courts have attempted to place restrictions on the subpoena to prevent  
21 Malibu from abusing the process to extort defendants, Malibu has flagrantly  
22 disregarded them. For example, after one court issued "two orders unambiguously  
23 ordering [Malibu] to file [the identified IP-registrant's name] under seal," Malibu  
24 filed it publicly anyway. Order to Show Cause, ECF Doc. No. 17, *Malibu Media,*  
25 *LLC v. Austen Downs*, 14-cv-707 (S.D. Ohio May 26, 2015). And in the Eastern  
26 District of New York, Magistrate Judge Gary Brown took additional precautions to  
27 protect John Doe's identity by explicitly instructing that "the subpoenaed  
28 information be sent directly to the Court, ex parte and under seal." *Patrick Collins,*  
*Inc. v. Doe 1*, 288 F.R.D. 233, 236 (E.D.N.Y. Nov. 20, 2012). Malibu instead  
served subpoenas that requested the identifying information be sent directly to  
Plaintiff's counsel. *Id.*

29 Despite these concerns, most district courts have permitted Plaintiff to serve ISPs with  
30 third-party subpoenas to discover the identity of the customer associated with the relevant IP  
31 Address. *See, e.g., Malibu Media, LLC v. John Doe*, No. 15-cv-4381 (JFK), 2015 WL 4923114  
32 (S.D.N.Y. Aug. 18, 2015); *Malibu Media, LLC v. John Does 1-16*, No. 12-cv-1847-AJB (DHB),  
33 2012 WL 3809128 (S.D. Cal. Sept. 4, 2012).<sup>2</sup> The service of these subpoenas, however, has been  
34 subject to restrictions aimed at protecting the privacy and the interests of the individuals whose  
35 identity is discovered pursuant to the subpoenas. With this interest-balancing framework in mind,

36  
37  
38 <sup>2</sup> Other district courts, however, have refused to grant Malibu Media's motion to serve a third-party subpoena. *See*  
*Malibu Media, LLC v. Doe*, No. 15-cv-4369, 2015 WL 4092417, at \*4-6 (S.D.N.Y. July 6, 2015); *Malibu Media, LLC*  
*v. Doe*, No. 15-cv-1883, 2015 WL 3651566, at \*2-4 (S.D.N.Y. June 5, 2015).

1 and particularly the concerns highlighted regarding these cases, the Court turns to Plaintiff's  
2 request to serve a third-party subpoena in this case and whether good cause exists to do so.

3 **2. Good Cause Factors**

4 In evaluating whether a plaintiff has established good cause to learn the identity of Doe  
5 defendants through early discovery, courts examine whether the plaintiff (1) identifies the Doe  
6 defendant with sufficient specificity that the court can determine that the defendant is a real person  
7 who can be sued in federal court, (2) recounts the steps previously taken to locate and identify the  
8 defendant, (3) demonstrates that the action can withstand a motion to dismiss, and (4) establishes  
9 that the discovery is likely to lead to identifying information that will permit service of process.  
10 *Columbia Ins. Co.*, 185 F.R.D. at 578-80; *Uber Technologies, Inc. v. Doe*, No. C 15-00908 LB,  
11 2015 WL 1205167, at \*2 (N.D. Cal. Mar. 16, 2015).

12 Here, Plaintiff has made a sufficient showing under each of the four factors to permit it to  
13 serve a third-party subpoena to identify Defendant.

14 **a. Sufficient Specificity and Recounting Steps to Identify Defendant**

15 Plaintiff has identified Defendant with sufficient specificity and has set forth the steps it  
16 has taken to do so. Its investigator Daniel Susac is employed by Excipio GmbH, a company that  
17 provides forensic investigation services to copyright owners. (Doc. 6-3, Susac Decl., ¶¶ 1-5.)  
18 Using forensic software, Susac was able to scan the BitTorrent file distribution network for the  
19 presence of infringing transactions involving Plaintiff's works. (Doc. 6-3, Susac Decl., ¶ 9.) A  
20 computer using the IP Address identified in Plaintiff's complaint connected to the investigator  
21 server to transmit a full copy, or portion, of the digital media files identified by the file hash values  
22 set forth in Exhibit A to the complaint.<sup>3</sup> (Doc. 6-3, Susac Decl., ¶ 11.) The IP Address  
23 identification is sufficient, at this stage, to indicate a real person used the network to download the  
24 copyrighted files. Moreover, Plaintiff sufficiently set forth the steps it has taken to locate and  
25 identify Defendant, despite that it has been unable to further identify Defendant by name. *See*  
26

27  
28 <sup>3</sup> Exhibit A contains a list of 137 file hash numbers associated with a particular copyrighted title and the date it was allegedly downloaded by Defendant. (Doc. 1-1, Exhibit A.)

1 *Hard Drive Prods., Inc. v. Does 1-118*, No. C 11-01567 LB, 2011 WL 1431612 (N.D. Cal. Apr.  
2 14, 2011). The first two good cause factors are satisfied.

3 **b. Sufficiency of Complaint to Withstand a Motion to Dismiss**

4 **(i) Ability to State a Claim Upon Which Relief Can Be Granted**

5 To be entitled to early discovery, Plaintiff must establish its complaint can withstand a  
6 motion to dismiss. *Columbia Ins.*, 185 F.R.D. at 579. "Copyright is a federal law protection  
7 provided to the authors of original works of authorship." *Vernor v. Autodesk, Inc.*, 621 F.3d 1102,  
8 1106 (9th Cir. 2010) (quoting 17 U.S.C. §§ 101-103). "To establish [copyright] infringement, two  
9 elements must be proven: (1) ownership of a valid copyright, and (2) copying of constituent  
10 elements of the work that are original." *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340,  
11 361 (1991). Plaintiff alleges it is the owner of the Copyrights-in-Suit (as identified in an exhibit to  
12 the complaint); using BitTorrent, Defendant copied and distributed constituent elements of each of  
13 the original works covered by the Copyrights-in-Suit; and Plaintiff did not permit or consent to  
14 Defendant's distribution of its works. (Doc. 1, ¶¶ 29-32.) It appears Plaintiff has stated a prima  
15 facie claim for copyright infringement that can withstand a motion to dismiss.

16 **(ii) Personal Jurisdiction**

17 Plaintiff bears the burden to establish jurisdictional facts, which includes personal  
18 jurisdiction over the defendant. *Columbia Ins.*, 185 F.R.D. at 579. Plaintiff has identified the IP  
19 Address associated with the allegedly infringing downloading and copying, and it is located in  
20 Sonora, California. This location is within the geographical boundaries of this judicial district.  
21 (Doc. 1, ¶ 5; Doc. 1-1, Exhibit A (identifying location of IP Address).) Further, the complaint  
22 alleges each of Defendant's acts of copyright infringement occurred in this district and that  
23 Defendant or its agents reside or may be found in this district. (Doc. 1, ¶ 7.) At this stage, it is  
24 likely that the complaint can withstand a motion to dismiss for lack of personal jurisdiction  
25 because Defendant has an IP Address traced to a location in this district. *See 808 Holdings v.*  
26 *Collective of December 29, 2011*, No. 12-cv-00186, 2012 WL 1648838 (S.D. Cal. May 4, 2012).



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**(iii) Venue**

"In copyright infringement actions, venue is proper 'in the district in which the defendant or his agent resides or may be found.'" *Brayton Purcell LLP v. Recordon & Recordon*, 606 F.3d 1124, 1128 (9th Cir. 2010) (quoting 28 U.S.C. §1400(a)). As noted above, Plaintiff has determined the alleged infringing activity occurred through an IP Address within this judicial district; thus, it is likely Plaintiff will be able to survive a motion to dismiss for improper venue under Federal Rule of Civil Procedure 12(b)(3). *See Malibu Media, LLC*, 2012 WL 3809128, at \*4-5.

**c. Subpoena Likely to Lead to Discovery of Identifying Information**

It appears Plaintiff has obtained and investigated the available data pertaining to the alleged infringements and there is no alternative means to ascertain Defendant's identity other than by subpoenaing the ISP. Doc. 6-1, 21:25-22:16; *see id.*, at \*3 (IP Addresses obtained sufficiently established investigation efforts, particularly where there is no other practical measures to identify Doe defendants). The information Plaintiff seeks through service of the subpoena will likely to lead to identifying information, including Defendant's name and address, which should allow Plaintiff to effect service of process on Defendant.

In sum, Plaintiff has made a sufficient showing on all four good cause factors to permit it to pursue discovery prior to the Rule 26(f) conference.

**3. Cable Privacy Act**

The Cable Privacy Act, 47 U.S.C. §551, generally prohibits cable operators from disclosing personally identifiable information regarding subscribers without the prior written or electronic consent of the subscriber. 47 U.S.C. §551(c)(1). The cable operator, however, may disclose this information if the disclosure is made pursuant to a court order and the cable operator provides the subscriber with notice of the order. *Id.* § 551(c)(2)(B). The ISP Plaintiff intends to subpoena is a cable operator within the meaning of the Act.

**4. Conclusion**

Based on the factors discussed above, the Court finds the privacy concerns of the Defendant are balanced with the need for discovery by allowing Malibu to subpoena the ISP to

1 discover Defendant's identity using the IP Address associated with the allegedly infringing  
2 downloads. The restrictions set forth below are intended to provide additional safeguards to  
3 Defendant's privacy interests. This Court takes very seriously the concerns noted by Judge  
4 Hellerstein of the Southern District of New York<sup>4</sup> and Judge Wright of the Central District of  
5 California,<sup>5</sup> among many others, regarding the potential for abuse in cases such as this. Although  
6 Plaintiff is permitted to serve a third-party subpoena, it is cautioned that any abuses of the judicial  
7 system or the discovery process will not be taken lightly.

#### 8 **IV. CONCLUSION AND ORDER**

9 On balance of the interests involved, the Court finds Plaintiff has established good cause  
10 for the issuance of a third-party subpoena in an attempt to identify Defendant. For the reasons set  
11 forth above, IT IS HEREBY ORDERED that:

12 1. Plaintiff's motion to serve a third-party subpoena is GRANTED subject to the  
13 restrictions noted below;

14 2. Plaintiff may immediately serve a Rule 45 Subpoena ("Subpoena") on AT&T  
15 Internet Services to obtain information to identify Defendant John Doe, specifically his or her  
16 name and address. The ISP is **not** to release the subscriber's telephone number or email address. A  
17 copy of this Order shall be attached to the Subpoena;

18 3. AT&T Internet Services shall have 60 days from the date of service of the  
19 Subpoena upon it to serve Defendant John Doe with a copy of the Subpoena and a copy of this  
20 Order. AT&T Internet Services may serve the Defendant using any reasonable means, including  
21 written notice sent to his or her last known address, transmitted either by first-class mail or via  
22 overnight service;

23 4. Defendant shall have 60 days from the date of service of the Subpoena and this  
24 Order upon him or her to file any motions with this Court contesting the Subpoena (including a  
25 motion to quash or modify the Subpoena), as well as any request to litigate the Subpoena  
26 anonymously. AT&T Internet Services may **not** turn over the Defendant's identifying information

27 <sup>4</sup> See *Malibu Media, LLC*, 2015 WL 4092417.

28 <sup>5</sup> See *Malibu Media, LLC*, 2012 WL 5382304.

1 to Plaintiff before the expiration of this 60-day period. Additionally, if the Defendant or ISP files  
2 a motion to quash the Subpoena, the ISP may not turn over any information to the Plaintiff until  
3 the issues have been addressed and the Court issues an Order instructing the ISP to resume turning  
4 over the requested discovery;

5         5.         If the 60-day periods elapse without the Defendant or ISP contesting the Subpoena,  
6 the ISP shall have 10 days to produce the information responsive to the Subpoena to Plaintiff. A  
7 Doe Defendant who moves to quash or modify the Subpoena, or to proceed anonymously, shall at  
8 the same time as her or his filing notify the ISP so that the ISP is on notice not to release any of  
9 the Defendant's contact information to Plaintiff until the Court rules on any such motions;

10         6.         AT&T Internet Services shall preserve any subpoenaed information pending the  
11 resolution of any timely-filed motion to quash; and

12         7.         Any information ultimately disclosed to Plaintiff in response to a Subpoena may be  
13 used by Plaintiff for the **sole** purpose of protecting Plaintiff's rights as set forth in the complaint.

14  
15 IT IS SO ORDERED.

16 Dated: March 18, 2016

/s/ Sheila K. Oberto  
UNITED STATES MAGISTRATE JUDGE

17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28