

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

|  |   |                                 |
|--|---|---------------------------------|
| MALIBU MEDIA, LLC,                         | ) |                                 |
|  | ) |                                 |
| <i>Plaintiff,</i>                          | ) | Civil No. 2:15-cv-03504-JFB-SIL |
|  | ) |                                 |
| v.   | ) |                                 |
|  | ) |                                 |
| JOHN DOE subscriber assigned to IP address | ) |                                 |
| 98.116.160.61                              | ) |                                 |
|  | ) |                                 |
| <i>Defendant.</i>                          | ) |                                 |
|  | ) |                                 |

**MOTION TO QUASH SUBPOENA AND MOTION FOR A PROTECTIVE  
ORDER BY DEFENDANT JOHN DOE**

Defendant, John Doe, by and through the undersigned counsel, files this Motion to Quash Subpoena and Motion for a Protective Order pursuant to Federal Rules of Civil Procedure 26 and 45 and would show as follows.

**I. INTRODUCTION & BACKGROUND**

1. On June 16, 2015, Plaintiff brought the instant suit in the Eastern District of New York against unnamed Defendant, who is identified only by Internet Protocol addresses, “IP Address 98.116.160.61.” (ECF Doc. 1).
2. On or about August 7, 2015, Defendant received a letter from the ISP informing him that the ISP had received a subpoena seeking documents identifying Defendant's name and address and that IP Address 98.116.160.61.was assigned to Defendant at 03:31:54 on May 23, 2015.
3. Defendant has not been served with any complaint.

4. Defendant did not copy or transmit Plaintiff's copyrighted works on May 23, 2015 at 03:31:54 and was not a part of Plaintiff's alleged BitTorrent "swarm."

5. This lawsuit against innocent Defendant is a part of the latest iteration of "a nationwide blizzard of civil actions brought by purveyors of pornographic films alleging copyright infringement by individuals utilizing a computer protocol known as "BitTorrent." *In Re: BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80, 82 (E.D.N.Y. 2012).

#### **A. BitTorrent**

6. BitTorrent is a peer-to-peer (P2P) 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") download 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. *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).

7. BitTorrent is distinguished 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.

## **B. Inconclusive Methods for Identifying Infringing BitTorrent Users**

8. A group of engineers in the University of Washington conducted a scientific, experimental study of monitoring and copyright enforcement on P2P file sharing and found that practically any Internet users can be framed for copyright infringement and even without being explicitly framed, innocent users may still be identified as an infringer even if they have never used P2P software. See *Challenges and Directions for Monitoring P2P File Sharing Networks-or- Why my Printer Received a DMCA Takedown Notice*, The University of Washington, available at <http://dmca.cs.washington.edu/>, last visited on September 23, 2015.

9. The research engineers were able to generate hundreds of real Digital Millennium Copyright act (DMCA) takedown notices for computers at the University of Washington that never downloaded nor shared any content whatsoever by profiling copyright enforcement in the BitTorrent file sharing system. Further, they were able to remotely generate complaints for nonsense devices including several printers and a wireless access point. The research results demonstrate several simple techniques that a malicious user could use to frame arbitrary IP addresses as network endpoints which are infringing the copyrights. *Id.*

10. In P2P filing sharing networks users are typically identified by the IP addresses of their computers. However, most ISPs today assign IP addresses to users dynamically (using the DHCP mechanism). The dynamic reassignment of IP addresses could result in users being falsely accused. *Id.*

11. The research concludes that the common approach for identifying infringing users in the poplar BitTorrent file sharing network is not conclusive. *Id.*

**C. Copyright Trolls**

12. Recent empirical studies show that the field of copyright litigation is increasingly being overtaken by “copyright trolls,” roughly defined as plaintiffs who are “more focused on the business of litigation than on selling a product or service or licensing their [copyrights] to third parties to sell a product or service.” Matthew Sag, *Copyright Trolling, An Empirical Study*, 100 Iowa L. Rev. 1105, 1108 (2015). “The paradigmatic troll plays a numbers game in which it targets hundreds or thousands of defendants, seeking quick settlements priced just low enough that it is less expensive for the defendant to pay the troll rather than defend the claim.” *Id.* The lawsuits most frequently target anonymous John Does for alleged infringement related to the use of BitTorrent. Indeed, of “the 3,817 copyright law suits filed in 2013, over 43% were against John Does and more than three-quarters of those related to pornography” *Id.* at 1108-09. But almost none ever reaches a hearing. Rather, the “lawsuits are filed to take advantage of court-ordered discovery [under Fed. R. Civ. P. 26(d)] to break the veil of anonymity that separates IP addresses from the account information of actual human 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.<sup>1</sup> *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

---

<sup>1</sup> Initially, these lawsuits attempted to join every Peer from a given BitTorrent Swarm in infringement actions, which is why the defendants in the captions are typically “John Does 1-X,” with X being a large number. However, over the past few years, judges in this District and others became hostile to mass joinder in these cases, characterizing the approach as an effort to circumvent the filing fees owed by Plaintiff. *See, e.g., Digital Sins, Inc. v. John Does 1-245*, 11-cv-8170, 2012 WL 1744838, at \*3 (S.D.N.Y. May 15, 2012) (Judge McMahon explaining that “[t]he only economy that litigating these cases as a single action would achieve is an economy to plaintiff — the economy of not having to pay a separate filing fee for each action brought.”). Facing higher costs, many of the most prominent filers seem to have ceased bringing large-scale “John Doe” actions. Remaining entities now sue each defendant individually.

and threatening phone calls.").

13. In 2012, judges in the Eastern District and across the country began awakening to the danger of copyright trolls, especially in the context of pornography. For example, 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." *Media Prods., Inc.*, No. 12-cv-3719 at 4 (S.D.N.Y. June 18, 2012). The largest copyright trolls were increasingly unscrupulous in abusing the litigation process to exploit this dynamic. *See In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80, 89 (E.D.N.Y. 2012) ("The most persuasive argument against permitting plaintiffs to proceed with early discovery arises from the clear indicia, both in this case and in related matters, that plaintiffs have employed abusive litigation tactics to extract settlements from John Defendants."); *Patrick Collins, Inc. v. Doe 1, Patrick Collins, Inc. v. John Does 1-37*, No. 12-cv-1259, 2012 WL 287832, at \*3 n.2 (C.D. Cal. Jul. 11, 2012) ("the federal courts are not flexible enough to be shaped into 'cogs in a plaintiffs copyright-enforcement business model. The Court will not idly watch what is essentially an extortion scheme, for a case that [Plaintiffs have] no intention of bringing to trial."); *Malibu Media, LLC v. Does 1-5*, 2012 WL 2001968, at \* 1 (S.D.N.Y. June 1, 2012) ("This Court shares the growing concern about unscrupulous tactics used by certain plaintiffs, especially in the adult films industry, to shake down the owners of specific IP addresses from which copyrighted adult films were allegedly downloaded."); *Digital Sins, Inc. v. John Does 1-245*, No. 11-cv-8170, 2012 WL 1744838, at \*3 (S.D.N.Y. May 15, 2012) ("In these BitTorrent cases, [ ] numerous courts have already chronicled abusive litigation practices ...."); *SBO Pictures, Inc. v. Does 1-20*, No. 12-cv-3925, 2012 WL 2034631, at \*1 (S.D.N.Y. June 5, 2012) ("Finally, early

quick settlement payments, regardless of their liability."); *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239,242 (S.D.N.Y. 2012) ("This course of conduct indicates that the plaintiffs have used the offices of the Court as an inexpensive means to gain the Defendants' personal information and coerce payment from them. The Plaintiffs seemingly have no interest in actually litigating the cases, but rather simply have used the Court and its subpoena powers to obtain sufficient information to shake down the John Does.").

14. These tactics, warned Judge Baer, "could turn copyright protection on its head." *Media Prods. Inc., DBA Devil 's Film v. John Does 1-26*, 12-cv-3719, at 4 (S.D.N.Y. June 18, 2012). In order to prevent that from happening, judges began attaching conditions to the various subpoenas they issued, but have found that plaintiffs often ignore them. *Malibu Media, LLC. V. John Doe*, 15-Civ-4369 (S.D.N.Y. July 6, 2015).

#### **D. Malibu Media, LLC**

15. Malibu Media, LLC is a California company owned by Collette Field and her husband, Brigham Field. The company produces erotic videos and distributes them through its subscription website, "X-art.com." Subscribers can obtain unlimited access to Malibu's pornographic video catalog for a monthly fee of \$24.95 or \$99.95 annually. (Field Decl. ¶12. ECF Doc 6.)

16. Malibu hires private investigators to seek out internet users who download or share Malibu-copyrighted videos, and brings lawsuits against them. Malibu is a prolific litigant: between January and May 2014, for example, Malibu was responsible for 38% of copyright lawsuits filed in the United States. Gabe Friedman, *The Biggest Filer of Copyright Lawsuits? This Erotica Web Site*, NEW YORKER, May 14, 2014, available at <http://www.newyorker.com/currency-tag/the->

biggest-filer-of-copyright-lawsuits-this-erotica-web-site. And the company has filed more copyright actions against John Defendants than any other plaintiff in each of the past three years. *See Sag, supra* at 1132.

17. Malibu spends much of its brief touting its integrity as a content-producer and distinguishing itself from copyright trolls. It cites comments by Judge Baylson during a 2013 "bellwether" trial in the Eastern District of Pennsylvania meant to test the viability of Malibu's claims. Judge Baylson stated that "Malibu is not what has been referred to in the media and legal publications, and in the internet blogosphere, as a 'copyright troll' ... Rather, Malibu is an actual producer of adult films and owns valid copyrights, registered with the United States Copyright Office, in its works." *Malibu Media, LLC v. John Does 1, 6, 13, 14*, Civ. A. 12-2078, 2013 WL 3038025 (E.D. Pa. June 18, 2013).

18. However, Malibu's corporate strategy relies on aggressively suing for infringement and obtaining accelerated discovery of the IP address holder's identity from the ISP. It then seeks quick, out-of-court settlements which, because they are hidden, raise serious questions about misuse of court procedure. Judges regularly complain about Malibu. For example, in May, the Honorable 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 that, while "Malibu Media asserts that it is necessary to invoke the Court's subpoena power to 'propound discovery in advance of a Rule 26(f) conference'. ..[,] not a single one of these 60 cases [filed in this district over the previous 12 months] has even progressed to a Rule 26(f) conference." *Id.* at 5. Indeed, most are dismissed even without the issuance of a summons. *Id.* Malibu's motive is to use the federal courts only to obtain identifying information in order to coerce fast settlements. *Id.* at 8 (citing *Malibu Media, LLC v. Does 1-54*, No. 12-cv-1407, 20 WL 30302, at \*5 (D. Colo. July 25,

*Media, LLC. V. John Doe subscriber assigned IP address 98.116.160.61*, 15-Civ-4369 (S.D.N.Y. July 6, 2015).

19. Malibu effectuates its strategy by employing tactics clearly calculated to embarrass defendants. For example, in recent complaints filed in the Wisconsin federal courts, an attached "Exhibit C" listed additional pornographic videos downloaded to the defendants' IP addresses using BitTorrent. The titles in Exhibit C were extremely racy and lewd, and the district court sanctioned Malibu when it learned that Malibu did not even own the copyrights for the titles; rather, it had gratuitously listed them to coerce larger, faster settlements by further shaming defendants. *See Malibu Media LLC v. John Doe subscriber assigned IP address 24.183.51.58, 2013 WL4821911* (W.D. Wis. Sep. 10, 2013); *Malibu Media, LLC 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 Malibu from abusing the process to extort defendants, Malibu has flagrantly disregarded them. For example, after one court issued "two orders unambiguously ordering [Malibu] to file [the identified IP-registrant's name] under seal," Malibu filed it publicly anyway. Order to Show Cause, ECF Doc. No. 17, *Malibu Media, LLC v. Austen Downs*, 14-cv-707 (S.D. Ohio May 26, 2015). And in the Eastern District of New York, Magistrate Judge Gary Brown took additional precautions to protect John Doe's identity by explicitly instructing that "the subpoenaed information be sent directly to the Court, ex parte and under seal." *Patrick Collins, Inc. v. Doe I*, 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.*



## E. Procedural History

21. Like almost all Malibu Media's cases, shortly after this one was filed, Plaintiff moved for leave to issue a third-party subpoena on the ISP, here, Verizon, which services the account identified by IP address "98.116.160.61" to identify the account's subscriber. This Court found "good cause" for the issuance of a subpoena. Movant, Defendant, asks that this Court, among other things, reconsider that finding of "good cause."

## II. Motion to Quash the Third Party Subpoena

### A. No "Good Cause"

22. Ordinarily, a "party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except in a proceeding exempt from initial disclosure under Rule 26(a)(1)(B), or when authorized by these rules, by stipulation, or by court order." Fed. R. Civ. P. 26(d)(1). The Court can order earlier discovery if the party seeking discovery shows "good cause." *Ayyash v. Bank Al-Madina*, 233 F.R.D. 325, 326 (S.D.N.Y. 2005). The following factors frame the "good cause" inquiry in cases of online copyright infringement:

(1) [the] concrete[ness of the plaintiffs] 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 v. Doe 3*, 604 F.3d 110, 119 (2d Cir. 2010) (quoting *Sony Music Entm't v. Does 1-40*, 326 F. Supp. 2d 556, 564-65 (S.D.N.Y. 2004)).

A pre-conference subpoena motion, like any "motion seeking a discovery ruling[,] is addressed to the discretion of the district court." *Baker v. F & F. Inv.*, 470 F.2d 778, 781 (2d Cir. 1972).

23. Plaintiff asserts that good cause exists to grant its motion to subpoena

Verizon, the internet service provider, because (a) it has established a *prima facie* claim for copyright infringement against Defendant; (b) it has clearly identified the specific information it seeks; (c) there is no other way to obtain Defendant's identity; (d) identifying the Defendant is necessary for Plaintiff to advance his claims; and (e) Defendant does not have a legitimate interest in remaining anonymous. In support of its motion, Malibu filed declarations by Collette Field, the owner of Malibu, and Patrick Paige, a former detective in the Palm Beach County Sheriff's Department who worked in the computer crimes unit.

24. However, on July 6, 2015, in a near-identical case, Judge Alvin K. Hellerstein of the Southern District of New York entered an order denying Malibu Media's motion for leave to serve a subpoena on Time Warner Cable. See *Malibu Media, LLC v. John Doe Subscriber assigned IP Address 66108.67.10*, 1:15-cv-04369-AKH (S.D.N.Y. July 2015).

25. In that case, Judge Hellerstein found that Malibu failed in establishing a *prima facie* claim.

26. A *prima facie* copyright infringement claim consists of two elements: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original. See *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc.* 499 U.S. 3400, 361 (1991).

27. As Judge Victor Marrero of the Southern District of New York observed in *Next Phase Distribution, Inc. v. John Does 1-27*, 284 F.R.D. 165, 171 (S.D.N.Y. 2012), "if the Motion Picture is considered obscene, it may not be eligible for copyright protection."

28. Further, even if Malibu's copyrights are valid, Malibu has not established a violation by the individual *to whom the relevant IP address is registered*. As Judge J. Paul Oetken of the Southern District of New York explains,

[t]he fact that a copyrighted work was illegally downloaded from a certain IP address does not necessarily mean that the owner of that IP address was the infringer. Indeed, the true infringer could just as easily

be a third party who had access to the internet connection, such as a son or daughter, houseguest, neighbor, or customer of a business offering internet connection.

*Patrick Collinc, Inc. v. Does 1-6*, No. 12-cv-2964, 2012 WL 2001957, at \*1 (S.D.N.Y. June 1, 2012); *see also In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80, 84 (E.D.N.Y. 2012) (“[T]he assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time.”); *Digital Sin, Inc. v. John Does 1-176*, 279 F.R.D. 239, 242 (S.D.N.Y. 2012) (Judge Nathan finding that approximately 30% of John Does identified by their internet service providers are not the individuals who actually downloaded the allegedly infringing films). The risk of misidentification is great in a world with ubiquitous Wi-Fi, and given courts’ concerns that these sorts of allegations —especially by this plaintiff—are likely to coerce even innocent defendants into settling, the risk of misidentification is important to protect against.” See *Malibu Media, LLC v. John Doe Subscriber assigned IP Address 66108.67.10*, 1:15-cv-04369-AKH (S.D.N.Y. July 2015).

29. And even if Plaintiff could definitively trace the BitTorrent activity in question to the IP-registrant Malibu conspicuously fails to present any evidence that John Doe either uploaded, downloaded, or even possessed a complete copyrighted video file. (*See* Compl. ¶19 (“IPP International UG downloaded from Defendant *one or more bits* of each file hash listed on Exhibit A.”) (emphasis added); Doc 8. Fieser Decl. ¶15 (“Our software downloaded one or more bits of each file hash listed on Exhibit A from the IP address referenced on Exhibit A.”)). Another district court has noted that

[i]ndividual BitTorrent file pieces are worthless ... If it is the case that a Doe Defendant logged onto the BitTorrent swarm, downloaded and then uploaded a single piece to the IPP server, and then logged off, all he has done is transmit an unusable fragment of the copyrighted work....[T]he Court notes that Malibu's case is weak if all it can prove is that the Doe Defendants transmitted only part of all the BitTorrent

*Malibu Media, LLC v. John Does 1-10*, No. 12-cv-3623, 2012 WL 5382304, at \*3 (C.D. Cal. June 27, 2012).

30. Plaintiff's assertion that there is no alternative means of obtaining the desired information is inadequate. The only support for it comes from the declaration of Patrick Paige who, as Magistrate Judge Kevin Nathaniel Fox of the Southern District of New York found, has no personal knowledge of what information "ISPs can use" or what procedures, if any, ISPs employ or the substantive work they perform in analyzing their data or identifying their subscribers. Paige also failed to establish any basis for his statement that "[t]he only entity able to correlate an IP address to a specific individual at a given date and time is the Internet Service Provider," given that he has never been employed by any ISP, and he does not claim he has personal knowledge of what methods, if any, are used by ISPs or any other entity to correlate an IP address to a specific individual at a given date and time. *Malibu Media, LLC v. John Doe subscriber assigned IP address 207.38.208.137*, 15-cv-1883, ECF Doc. No. 16 (S.D.N.Y. Apr.10, 2015); See also *Malibu Media, LLC v. John Doe Subscriber assigned IP Address 66108.67.10*, 1:15-cv-04369-AKH, ECF Doc. 10 (S.D.N.Y. July 06, 2015).

31. The Paige declaration that Judge Fox found deficient is identical to the Paige declaration submitted in support of the motion for this case.

32. For the reasons above, Malibu failed to establish "good cause."

33. Therefore, Defendant respectfully requests that the Court grant this motion to quash the third party subpoena.

#### **B. Undue Burden on Defendant**

34. Under Fed. R. Civ. P. 45(d)(3), the Court must quash or modify a subpoena

or subjects a person to an undue burden.”

35. Defendant did not copy or transmit Plaintiff’s copyrighted works and was not a part of Plaintiff’s alleged BitTorrent “swarm” on May 23, 2015 at 03:31:54 nor any other times.

**(1) IP Address might be Framed for Infringement by a Malicious Attacker**

36. As explained in ¶ 8 -11 above, there are many methods that may frame arbitrary IP addresses as the copyright infringing endpoints, leading the copyright enforcement lawsuits to many innocent internet users like Defendant.

37. In *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 241 (S.D.N.Y. 2012), Plaintiff’s counsel estimated that 30% of the names turned over by ISPs are not those of individuals who actually downloaded or shared copyrighted material.

38. According to the authors of *Challenges and Directions for Monitoring P2P File Sharing Networks-or- Why my Printer Received a DMCA Takedown Notice*, The University of Washington, available at <http://dmca.cs.washington.edu/>, last visited on September 23, 2015, the real perpetrator might turn out to be a malicious internet user who is in China or a neighbor in an apartment building.

39. Defendant strongly believes that his IP address was erroneously identified or wrongfully framed by an unknown internet user.

40. Also Defendant has been maintaining an open WIFI router to make the WIFI signal cover his house. This would increase the possibility of neighbors’ abuse of his IP address.

41. However, Malibu is seeking Defendant’s information only relying on the IP address, which is obtained by a method proved as inconclusive in the scientific research conducted by the University of Washington, *Id.*

42. If Defendant's identifying information is given to Plaintiff, Defendant will be subjected to the undue burden of proving third party's abuse of his IP address, which is practically impossible for Defendant given Defendant's limited knowledge on internet and BitTorrent even if his IP address was used by unknown malicious internet users.

## **(2) Extortion Strategy and Dynamic IP Address Assignment**

43. Malibu's strategy and its business models are to extort, harass, and embarrass defendants to persuade defendants to pay settlements with plaintiffs instead of paying for legal assistance while attempting to keep their anonymity and defending against allegations which can greatly damage their reputations.

44. Federal courts have addressed such practices regarding a plaintiffs "attempt to create a cottage industry of filing copyright claims, making large claims for damages and then settling claims for pennies on the dollar." *Righthaven LLC v. Democratic Underground LLC*, No. 2:11-cv-01356 (D. Nev. April 14, 2011). In this practice, "plaintiffs ... file cases with extremely weak infringement positions in order to settle ... and have no intention of taking a case to trial. Such a practice is an abuse of the judicial system and threatens the integrity of and respect for the courts." *Raylon, L.LC. v. EZ Tag Corp.*, No. 6:09-cv-00357 (E.D. Tex. March 9, 2011).

45. Further, Malibu is using a tactic to press defendants by increasing the number of total claims against a defendant, disregarding the nature of the IP address assignment mechanism.

46. IP addresses can be either dynamic or static. ISPs assign dynamic IP addresses to a computer for only as long as the current user's internet session lasts; a new IP address is assigned for each subsequent internet session. Static IP addresses do not change; the same number is assigned to the same computer consistently over time. Frederick Lah, *Are IP Addresses "Personally Identifiable Information"?* 4:3 *Journal of Law and Policy for the Information Society*

47. As a subscriber of Verizon Internet Services, Defendant's computer system also gets different IP addresses whenever it starts a new session.

48. Malibu claims in its Complaint against Defendant that it has identified the IP address (98.116.160.61) responsible for eighteen counts of copyright infringements from February 10 through May 23, 2015 (ECF Doc. 1).

49. The IP address (98.116.160.61) might have been assigned to eighteen different subscribers of Verizon because of the nature of dynamic IP assignment.

50. However, Malibu has issued a subpoena to Verizon asking the identity of a user of the IP address, 98.116.160.61, only at 03:31:54 on May 23, 2015.

51. Since Defendant's IP addresses were assigned dynamically by the ISP, even if Defendant was identified as the subscriber assigned the IP address, 98.116.160.61, at 03:31:54 on May 23, 2015, it doesn't mean that Defendant is the same subscriber who assigned the IP address at the other seventeen occasions.

52. No evidence was submitted by Malibu that is proving the subscriber of the IP address at 03:31:54 on May 23, 2015 is the same subscriber of the other seventeen occasions.

53. If Defendant's identifying information is given to Plaintiff, Plaintiff, as part of their business model, will seek settlements of thousands of dollars claiming Defendant's responsibility for eighteen downloads of copyright protected works under the threat of litigation and public exposure with no serious intention of naming Defendant.

54. Such an undue burden should be not shouldered by Defendant as the costs to Defendant clearly outweigh the frivolous and non-existent benefits of Plaintiff's claim, given their practice of judicial system abuse and the nature of these suits.

55. Therefore, Defendant respectfully requests that the Court grant this motion to

### III. Motion for Protective Order

56. Under Fed. R. Civ. P. 26 (c), the Court may, for good cause, issue an order to protect a party or person from “annoyance, embarrassment, oppression, or undue burden or expense.”

57. Good cause exists for a protective order to prevent the disclosure of Defendant’s identifying information because the disclosure of Defendant’s identifying information would subject Defendant to the annoyance, embarrassment, oppression, and undue burden and expense of being subject to Plaintiff’s attempt to try to extract a settlement out of Defendant.

58. Where a subpoena’s primary purpose is not to obtain information for use in the litigation but rather to extract money from numerous individuals, any request to identify such individuals is an undue burden. The subscribers, often embarrassed about the prospect of being named in a suit involving pornographic movies, settle. *MCGIP, LLC v. Doe*, 2011 WL 4352110, (N.D. Cal. September 16, 2011).

59. Courts have recognized that in these recent mass-Doe cases based on BitTorrent, “plaintiffs have used the offices of the Court as an inexpensive means to gain the Doe defendants’ personal information and coerce payment from them.” *K-Beech, Inc. v. Does 1-85*, No.3: 11cv469-JAG (E.D. Va. October 5, 2011).

60. Even if Plaintiff had a legitimate claim, their interests do not outweigh the interests of Defendant given the nature of their practice, and the Court may allow to proceed with Defendant remaining anonymous.

61. For these reasons, Defendant’s identifying information is not relevant to the litigation and disclosure of the same would subject Defendant to the harassment of multiple demands



62. Therefore, Defendant respectfully requests that the Court grant this motion  
and enter a protective order for Defendant's identity pursuant to Fed. R. Civ. P. 26 (c).

## VI. CONCLUSION

63. Plaintiff has failed to show "good cause" for the expedited discovery because  
it couldn't establish a *prima facie* claim and its claim that there is no alternative means of obtaining  
the desired information was inadequate. Also Plaintiff's third party subpoena unduly burdens  
Defendant because Defendant will be an innocent victim of Plaintiff's systematic attempt to leverage  
settlements from Defendant without valid claims and intent to bring to trial.

WHEREFORE, for the foregoing reasons, Defendant, "John Doe," respectfully requests that this  
Honorable Court enter an Order GRANTING this Motion and

1. QUASHING the outstanding subpoena seeking John Doe's identity;
2. ENTERING a protective order preventing Plaintiff from obtaining further discovery as to  
Defendant; and
3. FOR SUCH OTHER AND FURTHER RELIEF that this Court deems just and proper.

Dated: September 28, 2015

Respectfully submitted,

By: /s/Chejin Park  
Chejin Park  
NY Bar No. 4509063  
[cjparklawyer@gmail.com](mailto:cjparklawyer@gmail.com)  
Law Offices of Chejin Park PC  
35-20 147<sup>th</sup> Street, Suite 2C  
Flushing, NY 11354

**CERTIFICATE OF GOOD-FAITH CONFERENCE**

I hereby certify that, on September 28, 2015, I conferred, telephonically, with counsel for Plaintiff, who stated that Plaintiff is opposed to the relief requested in this motion.

By: /s/Chejin Park  
Chejin Park  
NY Bar No. 4509063  
Law Offices of Chejin Park PC  
35-20 147<sup>th</sup> Street, Suite 2C  
Flushing, NY 11354

**CERTIFICATE OF SERVICE**

I hereby certify that on September 28, 2015, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF and that service was perfected on all counsel of record and interested parties through this system.

By: /s/Chejin Park  
Chejin Park  
NY Bar No. 4509063  
Law Offices of Chejin Park PC  
35-20 147<sup>th</sup> Street, Suite 2C  
Flushing, NY 11354