UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC, Plaintiff, vs. JOHN DOE subscriber assigned IP Address 68.80.134.5, Defendant.	Case No. 2:15-cv-06337-CMR

PLAINTIFF'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO QUASH

Plaintiff, Malibu Media, LLC ("Plaintiff"), by and through undersigned counsel, files the instant response to Defendant John Doe's ("Defendant") Motion to Quash ("Defendant's Motion") [CM/ECF 6].

I. INTRODUCTION

Plaintiff's constitutional right under the Petition Clause to seek redress for the online infringement of its copyrights is at issue. Without the ability to obtain a subscriber's identity in an online infringement case, there is no remedy for online copyright infringement. Granting Defendant's motion to quash would be inconsistent with the Copyright Act, congressional intent, Third Circuit precedent, and the nearly universal opinion of district court judges around the country. The Court need not do so, however, because, as explained below, none of Defendant's three arguments to support his request have merit. Stated simply, Defendant's Motion fails to assert a legally cognizable reason to quash a subpoena under Rule 45.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

II. LEGAL STANDARD

At issue is Defendant's request that the Court quash the Rule 45 subpoena directed at Defendant's internet service provider. This request is governed by Rule 45(d)(3) which sets forth six limited situations under which a subpoena may be quashed (or modified): (1) if the subpoena "fails to allow a reasonable time to comply"; (2) if the subpoena requires a non-party to travel more than 100 miles (except for trial within the state); (3) if the subpoena requires disclosure of privileged materials; (4) if the subpoena subjects a person to "undue burden"; (5) if the subpoena requires disclosure of "a trade secret or other confidential research, development, or commercial information"; or (6) if the subpoena requires disclosure of certain expert opinions. *See* Fed. R. Civ. P. 45(d)(3)(A)–(B). The six circumstances enumerated in Rule 45(d)(3) are the **only** permissible circumstances under which a motion to quash may be granted. *See* Fed. R. Civ. P. 45(d)(3)(A)–(B); *Malibu Media, LLC v. John Does*, No. 12-cv-03170, 2013 WL 1164867, *2 (D. Colo. Mar. 20, 2013) (denying a motion to quash in a similar action under similar circumstances, emphasizing: "no other grounds are listed"); *Malibu Media, LLC v. Doe*, No. JKB-13-512, 2013 WL 6577039, *1 (D. Md. Dec. 12, 2013) (same); *Malibu Media, LLC v. John Does 1–9*, No. 8:12-cv-00669, CM/ECF 25 (M.D. Fla. July 6, 2012) (same).

III. ARGUMENT

A. Even if Defendant—the Subscriber Assigned the IP Address Used to Infringe Plaintiff's Copyrights—Is Not the Infringer, the Subpoenaed Information Remains Relevant and Discoverable

Although Defendant does not actually deny using his Internet to infringe Plaintiff's copyrights, he asks the Court to foreclose Plaintiff from proceeding with its claims since, at this point, it has not discovered evidence to exclude the possibility of a third-party infringer. As Defendant explains, any person of his household "would have unrestricted internet access," such

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

that pinpointing Defendant, as opposed to his family members, as the actual infringer "is guessing." CM/ECF 6 at p. 2. This argument fails; while Defendant is very likely the infringer, even if someone else used Defendant's Internet to infringe Plaintiff's copyrights—a consideration that is entirely premature at this stage of the litigation—Defendant's identity remains relevant and discoverable under the Federal Rules.

Identifying Defendant, the subscriber of the infringing IP address, is the only way to identify the infringer; even if Defendant is not responsible, he likely possesses information that will assist Plaintiff in identifying who is. This is extremely well-settled; courts repeatedly and uniformly instruct that the possibility that an internet subscriber is not the actual infringer is not a sufficient basis for quashing a Rule 45 subpoena. *See, e.g.*, *Malibu Media, LLC v. Does*, No. CIV.A. 12-07789 KM, 2014 WL 229295, at *8–9 (D.N.J. Jan. 21, 2014) ("The appropriate inquiry … is … whether the information sought reasonably leads to the discovery of admissible evidence. [I]t is possible that the Internet subscriber did not download the infringing material. It is also possible, however, that the subscriber either knows, or has additional information which could lead to the identification of the alleged infringer. If any defendant could quash a subpoena based on the mere possibility that someone else has used the defendant subscriber's IP address to perpetuate the alleged infringement, then a plaintiff would be unable to enforce its rights."); *see also Malibu Media, LLC v. Doe*, No. 15-1742, 2015 WL 5996319, at *2 (D. N.J. Oct. 14, 2015) (same); *Malibu Media, LLC v. Doe*, No. CIV.A. 14-3945 MAS, 2015 WL 3795716, at *4 (D. N.J. June 18, 2015) (same); *Malibu Media, LLC v. Doe*, No. 13 C 8484, 2014 WL 1228383, *2 (N.D. Ill. Mar. 24, 2014) (same); *TCYK, LLC v. Does*, No. 2:13-cv-539, 2013 WL 4805022, *4 (S.D. Ohio Sept. 9, 2013) (same); *Malibu Media, LLC v. Doe*, 2013 WL 5876192 (E.D. Wis. 2013) (same).

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

B. Defendant Does Not Have a Reasonable Expectation of Privacy in the Subpoenaed Information Pursuant to Rule 45(d)(3)(A)(iii)

Defendant's second argument is that an order quashing the Rule 45 subpoena is needed to prevent disclosure of private and sensitive information. Defendant bizarrely asserts, without any support or explanation, that failure to quash the Rule 45 subpoena may expose his "credit card information, purchase history, medical documents, appointments, job searches, as well as social media contacts…." CM/ECF 6 at p. 2. This argument is without any factual support whatsoever and should be rejected outright. To be sure, Plaintiff has only requested—and the Court has only authorized—issuance of a subpoena to learn Defendant's true name and address. *See* CM/ECF 4–5. This information, which is necessary for Plaintiff to effectuate service of process and proceed with this suit, is the only information that Plaintiff will obtain.

Further, Defendant's privacy argument is foreclosed by well-established law. "Courts have consistently ruled that Internet subscribers do not have a reasonable expectation of privacy in their subscriber information. This is because Internet subscribers have already voluntarily conveyed their subscriber information—name, address, and phone number to their Internet Service Provider. … Accordingly, [BitTorrent copyright infringement defendants] cannot now claim that such information is so confidential as to establish a basis for quashing a subpoena." *Malibu Media, LLC v. John Does 1-18*, No. CIV.A. 12-07789 KM, 2014 WL 229295, at *6–7 (D. N.J. Jan. 21, 2014); *see also Malibu Media, LLC v. Doe*, No. CIV.A. 14-3945 MAS, 2015 WL 3795716, at *3 (D. N.J. June 18, 2015) (denying motion to quash and rejecting argument that the defendant's "identifying information is so confidential as to establish a basis for quashing the subpoena"); *Malibu Media, LLC v. Does*, No. 1:12-cv-263, 2012 WL 6019259, *4 (N.D. Ind. Dec. 3, 2012) ("there is no expectation of privacy in Internet subscriber information because it has already been exposed to a third party, the Internet Service Provider. … Doe's

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

argument that fulfilling the subpoena would invade his privacy and jeopardize his identity is insufficient to quash the subpoena as he has no expectation of privacy in the identifying information the subpoena seeks from the ISP."); *Raw Films, Ltd. V. John Does 1-15*, No. 11-7248, 2012 WL 1019067, *8 (E.D. Pa. Mar. 26, 2012) (holding that individuals who use the internet to illegally copy and distribute copyrighted material have a minimal expectation of privacy since they "have already voluntarily given up certain information by engaging in that behavior").

C. To The Extent Defendant's *Ad Hominem* Attack Purports to Assert "Undue Burden" Under Rule 45(d)(3)(iv), He Lacks Standing

Defendant's final argument is that he has googled Plaintiff and formed a belief that Plaintiff will inundate him with phone calls and letters urging him to settle. *See* CM/ECF 6 at p. 1–2. Presumably, Defendant's argument is that the quashing the subpoena is necessary to avoid subjecting him to undue burden. This argument is factually and legally untenable.

Factually, Defendant will not be exposed to any sort of burden and Plaintiff will not harass Defendant to settle. Other than vaguely referring to google, Defendant does not identify the source of the any information that would leave him to believe otherwise. Truth be told, Defendant's allegations appear to be entirely fabricated insofar as Plaintiff never calls defendants to discuss settlement, nor does it ever even initiate settlement discussions with defendants prior to service of process. To urge this Court to infer otherwise, Defendant refers to an outlier opinion from the Southern District of Ohio, wherein one judge, concerned about so-called copyright trolls and less familiar with Plaintiff, opined that Plaintiff might engage in abusive litigation tactics. *See* CM/ECF 6 at p. 2–3. Plaintiff respectfully disagrees with that commentary and submits that it is erroneous. Indeed, following an extensive trial, this Court ruled that Plaintiff is not likely to abuse the process and that the criticism attributed to "copyright trolls" is

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming inter-face) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.