UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No.: 0:14-cv-60681-UU

MALIBU MEDIA, LLC,

Plaintiff,

v.

JOHN DOE SUBSCRIBER ASSIGNED IP ADDRESS 66.229.166.251,

Defendant.

_____/

ORDER TO SHOW CAUSE

THIS CAUSE comes before the Court upon a *sua sponte* review of the record.

THE COURT has reviewed the pertinent portions of the record, and is otherwise fully advised on the premises.

On March 18, 2014, Malibu Media, LLC, ("Plaintiff") commenced the instant action, alleging that an unknown Defendant utilized an Internet protocol called BitTorrent to infringe certain of Plaintiff's copyrights. D.E. 1.

The Eleventh Circuit has held that a district court may dismiss a suit *sua sponte* for lack of venue after giving the parties an opportunity to present their views on the issue. *Algodonera De Las Cabezas, S.A. v. Am. Suisse Capital, Inc.*, 432 F.3d 1343, 1345 (11th Cir. 2005) (quoting *Lipofsky v. New York State Workers Comp. Bd.*, 861 F.2d 1257 (11th Cir. 1988)). In the present case, the court questions whether venue is proper in this district for the reasons herein stated, and accordingly provides parties the opportunity to show why this case should not be dismissed for

improper venue.

Plaintiff's complaint asserts that venue in the Southern District is proper under 28 U.S.C. § 1391(c) and § 1400 (a) because Defendant resides in this District and State, and under U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in this District. D.E. 1. Plaintiff used geolocation technology to trace the copyright infringement to an Internet Protocol address ("IP address") located within this district. *Id.* Plaintiff's assertions as to Defendant's residency therefore seem to be in large part based upon the assumption that the geographic data results of IP address geolocation are valid and accurate. The Court is unpersuaded after reviewing technical literature which suggests otherwise.

Among the many challenges presented by the Internet is that the Internet itself possesses no inherent mechanism for determining the geographic location of connected devices. While Domain Name System (DNS) entries can include a location record, there is no standard protocol to provide global location data which corresponds with an Internet Protocol (IP) address. Brian Eriksson, Paul Barford, Joel Sommers & Robert Nowak, A Learning-Based Approach for IP Geolocation, Proc. of the Eleventh Int'l Conf. on Passive & Active Measurement (Zurich, Switz.), Apr. 7–9, 2010. Furthermore, the size and complexity of the Internet coupled with its highly diffuse ownership and user-base provides no single repository or authority which could maintain such data. Brian Eriksson, Paul Barford, Bruce Maggs & Robert Nowak, Posit: A Lightweight Approach for IP Geolocation, Submitted to SIGMETRICS Performance Evaluation Review Dec. 2011. Instead, IP address geolocation technologies rely primarily upon active network measurements, or alternatively databases of IP to location mappings. Phillipa Gill, Yasgar Ganjali, Bernard Wong & David Lie, Dude, Where's That IP? Circumventing Measurement-Based IP Geolocation, Proc. of the Nineteenth USENIX Conf. on Security (D.C.),

Aug. 11–13, 2010. The former falls victim to inconsistent Internet topology and incomplete information regarding this topology due to the Internet's rapid and continuous expansion. Anukool Lakhina, John W. Byers, Mark Crovella, Ibrahim Matta, On the Geographic Location of Internet Resources, IEEE J. on Selected Areas in Comm., Spec. Issue on Internet and WWW Measurement, Mapping, and Modeling, 2003. Similarly, databases of IP location mappings tend to be rough and incomplete—also due to the Internet's rapid expansion. Yong Wang, Daniel Burgener, Marcel Flores, Aleksandar Kuzmanovic & Cheng Huang, Towards Street-Level Client-Independent IP Geolocation, Proc. of the Eighth USENIX Conf. on Networked Systems Design & Implementation (Bos., Mass.), Mar. 30–Apr. 1, 2011.

Thus, despite the existence of geolocation software designed to approximate the geographical location of Internet-connected devices, this Court cannot rely solely upon Plaintiff's assertion that such technology was used for purposes of establishing proper jurisdiction and venue. This is particularly true in instances where 28 U.S.C. § 1400(a), the exclusive venue statute for copyright infringement, controls and permits venue to be laid in the district where the defendant resides or may be found.

For this Court to rely upon the use of geolocation for establishing proper venue, far more than mere conclusory statements by the Plaintiff is required. To allow this case to proceed in the Southern District, this Court requires a showing of the precise methodology and technique employed by the Plaintiff in its use of geolocation to establish—to a reasonable degree of certainty—that the Defendant may be found within this district.

Additionally, this Court recognizes that IP addresses are assigned to nodes connected to

the Internet, but are not necessarily representative of individual end-node/end-system devices,[1] and especially are not representative of individual people. This Court therefore requires that the Plaintiff show that due diligence, as well as due care, have been employed in ascertaining that the IP address associated with the alleged tortfeasor is or was[2] assigned to a system or node that can be used to reasonably calculate the identity[3] of the alleged infringing party.[4] Accordingly, it is hereby

ORDERED AND ADJUDGED that Plaintiff SHALL show cause, in fewer than twelve pages, why this Court may reasonably rely upon the Plaintiff's usage of geolocation or other technologies to establish the identity of the Defendant and that the Defendant may be found within this district ("Geolocation reliance question"). Mere speculation and conjecture will not suffice. Additionally, Plaintiff shall show cause why this case should not be dismissed *sua sponte* for improper venue ("Venue question"). Plaintiff shall respond to both questions by **Thursday,**

---

[1] In the hierarchical architecture of the Internet, end-nodes—also known as end-systems—can take an extraordinary number of forms due to the increasing number of electronic devices which are digitally interconnected using one or more of the Internet Protocol Suite communication control protocols. Common examples include personal computers and smartphones, but may also include IP/Wi-Fi security cameras, televisions, and high-tech household appliances. It is imperative that one recognize that a publicly-viewable IP address may represent nothing more than a router or gateway through which other devices connect. These devices, which may be part of a large intranet, may have their own private IP addresses that are not visible to users of the Internet outside of the intranet to which the device is connected.

[2] In the event of an IP address being assigned by a Dynamic Host Configuration Protocol (DHCP) server, a communication endpoint frequently may be assigned a new IP address. Dynamic versus static IP addresses are commonly used by Internet Service Providers to manage the shortage of IPv4 addresses—a problem which continues today due to the lack of IPv6 adoption.

[3] Additional impediments to establishing identity include proxy servers. Of particular note are public proxy servers and Common Gateway Interface (CGI) proxy servers—intended in some instances to specifically provide anonymity to torrent seeds (peers in possession of all data belonging to a shared data file) and downloaders. Similarly, the possibility of IP address spoofing is of concern and should not be ignored.

[4] For example: An IP address assigned to a personal computer located within a single occupancy residence is far more likely to be fruitful than an IP address assigned to a publicly accessible Wi-Fi router at a coffee-shop.

March 27, 2014.

DONE AND ORDERED in Chambers at Miami, Florida, this 20th day of March, 2014.

UNITED STATES DISTRICT JUDGE

copies provided: counsel of record
Magistrate Judge Torres