John C. Lowe
John Lowe, P.C.
5920 Searl Terrace
Bethesda MD 20816

Phone 202-251-0437
Fax 301•320•8878
EMAIL: JOHNLOWE@JOHNLOWEPC.COM

March 18, 2013

Hon. Roger W. Titus
Hon. Paul W. Grimm
U.S. District Court for the District of Maryland
6500 Cherrywood Lane
Greenbelt, MD 20770

March 25 Hearing about Malibu Media, LLC copyright cases.

Dear Judges Titus and Grimm:

I am a Virginia lawyer who has practiced as a trial lawyer in Maryland, Virginia, and the District of Columbia for over 45 years. I am co-counsel for Defendants in three of the pornographic film company copyright cases in your Court. [1] On behalf of my co-counsel I am accepting your invitation to send a letter and participate as amici curiae for the March 25 hearing. **I ask to be heard orally at the hearing, as well.**

The single most important point is that the plaintiffs, in these cases alleging copyright violations by down loading, copying, and distributing copyrighted pornographic movie films from the Internet, **cannot** prove who did the down loading, even if it actually occurred.

Among the defense expert witnesses in all three these cases is John Simek, Vice President of Sensei Enterprises, Inc., of Fairfax, VA, one of the top computer forensics companies in this part of the country. He has already given expert declarations in support of the three cases I have cited at fn 1. His declaration and CV in the Steinruck case in this Court is at CA 12-0347, Docket Number 57, and I incorporate that declaration and his CV into this letter by reference, as it is available to the Court in that case file.

As John Simek attests in his declaration in the Steinruck case -- the infringements alleged in these suits could be activities of third parties – neighbors in their own homes or persons with a laptop computers sitting in their pickup trucks up to 200 feet away from the house of the router

---

1 *Metro Media Entertainment, LLC v. Steinruck*, CA 12-0347
Third Degree Films, Inc., v. Barr, CA 12-0349
Third Degree Films, Inc. v. Osburn, CA 12-01294

owner – which infringing third parties are unknown and unknowable to the innocent router owner. [2] That is why it is crucial to understand that the Plaintiff in these cases cannot even prove what kind of device – a computer, for example – was used to down load the film. And when I have confronted Plaintiff's counsel in these cases about that fact, the response is a vague, "Well it probably is the router owner, because he is the one most likely to do it." – with no facts to support the premise.

In these cases, ordinary innocent citizens are met with a demand for money to avoid the humiliation and harm of being publicly named as a defendant in a suit by a pornographic film company. Regardless of how innocent they may be, few can afford to retain a lawyer or pay for the cost of litigation in order to defend themselves. Many pay the extortionate demands of the porn company plaintiffs as the lesser of two evils facing them. [3] The porn film companies count on that reality as source of undeserved money – and lots of it.

One of the proofs I offer to the characterization of these suits as merely shake downs is that with an estimate of over 200,000 John Doe Defendants nationwide, I have been unable to find a single John Doe copyright case in any court that has ever been taken to trial. I have asked every chance I get but no one knows of a single case. Porn company plaintiffs eventually just dismiss everyone who doesn't pay up, since they are more trouble than they are worth.

At the March 25 hearing it would be helpful for the Court to ask Plaintiff how they will prove who the infringing *person* was – not merely prove what router IP address was used by someone as a means of down loading the film (assuming that it took place at all – not a spoof). [4]

---

[2] There is a password associated with wireless routers designed to limit access to the Internet. However, the passwords are easily defeated by amateur hackers. Indeed, the Internet has all kinds of free software available on line that will defeat such password protection.

[3] At least two respected federal judges have stated on the record their assessment that the so-called settlement demands in similar suits before them brought by pornographic film companies, are extortion and shake downs. See e.g., *Patrick Collins, Inc. v. John Doe 1*. CA 12-1154 (SDNY, 2012)("shake down"; "extortion scheme"; *K-Beech, Inc. v. Does 1-85*, CA11 – 00469 (EDVA 2011)("shake down").

[4] A Plaintiff's counsel in a similar case admitted in federal court in New York that at least 30% of the defendants sued were not the persons who did the infringing. As New York federal Judge Alison J. Nathan said in an opinion in that case January 2012, "The Court is concerned about the possibility that many of the names and addresses produced in response to Plaintiffs discovery request will not in fact be those of the individuals who downloaded "My Little Panties #2." The risk is not purely speculative; Plaintiff's counsel estimated that 30% of the names turned over by ISPs are [4 (cont'd)] not those of individuals who actually downloaded or shared copyrighted material. Counsel stated that the true offender is often the "teenaged son ... or the boyfriend if it's a lady." . . . Alternatively, the perpetrator might turn out to be a neighbor in an apartment building that uses shared IP addresses or a dormitory that uses shared wireless networks." *Digital Sin, Inc. v. John Does 1-176*, 12 cv-00126 – AJN (SDNY 2012).

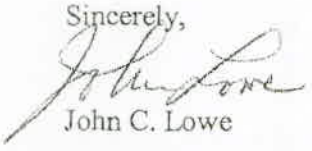
Another important reality is that, with modern Internet technology, virtually anyone can "spoof" any IP address or addresses. [5] That is to say, one can spoof an IP address and make it appear that it was used to down load a film from the Bit Torrent Network, while the down load was actually carried out by the hacker setting up the situation in a completely different location.

We have proved and can demonstrate to the Court at any time, upon request if desired, that a hacker located at a remote location -- the courtroom, for example -- can run an IP spoof targeting Dallas, Texas, for example, to make it appear that a Dallas, Texas IP address is illegally down loading a film from the Bit Torrent Network on a router far away from the hacker, when actually the down loading is occurring in the court room and there is no down loading of the film taking place at the Dallas, Texas IP address. This will be accomplished in such a way that the Bit Torrent Network will report that the down load was accomplished by a spoofed IP address in Dallas, Texas, a different location from the spoofing computer.

To describe this in simple and relevant terms, I say that Harry the Internet Hacker – the agent of mischief – can sit in Chatsworth, California, and down load a Malibu Media porn film, and spoof it so the Bit Torrent Network erroneously reports that an IP address owned by a John Doe in Waldorf, Maryland, was the party who down loaded the film, whereas the innocent owner of the router assigned that IP address in Waldorf has no idea this is going on and there will be no down load and no track left to tell the Maryland router owner what took place. This spoofing activity will generate all the data and documents filed by these porn film company Plaintiffs with their Complaints against those innocent John Does.

Again, I would like to speak at the hearing and would be happy to answer questions about the content of this letter.

Sincerely,



John C. Lowe

---

[5] Spoofing is successfully masquerading a computer as a different computer. IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged IP address, with the purpose of concealing the identity of the sender or impersonating another computer. So, for example, we recently successfully conducted a live demonstration where we caused a laptop in Reston, VA, to masquerade as a computer in Dallas Texas with a Dallas, Texas IP address, so any down loading activity by our Reston computer at that time would be registered as having been a down load by that Dallas, Texas computer. Anyone investigating the down load would find records that it was downloaded in Dallas, Texas, not Reston, VA.