IN THE UNITED STATES DISTRICT COURT FOR THE

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

HARD DRIVE PRODUCTIONS, INC.,
Plaintiff

v. Case No. C 11-01567 LB

DOES 1-118,
Defendants

MOTION TO QUASH OR MODIFY SUBPOENA

I, John Doe (72.129.105.245), file this motion to quash the subpoena served to Time Warner Cable, my Internet Service Provider (ISP), granting HARD DRIVE PRODUCTIONS, INC.'s application for leave to take discovery prior to rule 26(f) conference with extended joinder discussion. A copy of this motion will be provided to both the Court, my IS Provider and the Plaintiff.

The case against Does 1-118 is a strategic campaign by Plaintiff to coerce innocent people to settle out of court for thousands of dollars each to avoid embarrassment due to the association with this company's products (i.e., pornography). It is a "reverse class action" suit where Plaintiff wishes, by the cheapest means possible, to accuse huge numbers of unknown, innocent, and legally unknowledgeable people into litigation based

upon unreliable and limited information, and then "sort out" the real perpetrators after the fact. This imposes an unfair cost and burden on numerous innocent defendants, which Plaintiff uses to its advantage, to obtain unscrupulous settlements. Plaintiff's counsel, Steele Hansmeier and its associates, have filed a multitude of similar lawsuits alleging copyright infringement through BitTorrent. In Illinois and the Northern District of California alone, these accused defendants number in the tens of thousands.

To preserve my good name, I respond as John Doe, and ask that the Court permit me to proceed anonymously and prevent Plaintiff from obtaining exactly what they want: my name and contact information. This case should be dismissed immediately based on the following statements:

1) Improper Joinder of Parties.

The claims against me qualify as a unique case. Does 1-118 all have completely different network configurations both at the ISP and the personal home network level. Each individual Doe deserves a right to an individual investigation with individual accusal and defense. Joinder requires that each case share sufficient overlap to be grouped together. In this case, each Doe relies on entirely separate network configurations and computer and network hardware; as a result, this case does not qualify. If allowed to proceed, this would be a gross misuse of joinder.

Moreover, the list of Does 1-118's alleged activities as submitted by Plaintiff covers the dates from March 9, 2011 to March 29, 2011, a period of nearly three weeks. This time span calls into question if there was ever common "concerted" activity linking all 118 IP addresses in this case as claimed by Plaintiff. It is difficult to believe that any or all of the Does would patiently wait three weeks for all the pieces of the copyrighted work to be gathered together so that it could be watched as a whole.

Joinder based on separate but similar behavior by individuals allegedly using the Internet to commit copyright infringement has been rejected by courts across the country.

A: *Pacific Century International Ltd., v. Does 1-101* (4:11-cv-02533-DMR)

Judge Donna Ryu held that it is improper to sue BitTorrent users from different swarms in the same copyright infringement lawsuit, even if they all downloaded the same copyrighted work (e.g., the same movie). For example, in one swarm, the users may download a low quality version of the movie and in another swarm, a different set of users may download a high quality version of the same movie. Judge Ryu ruled that is improper to join the first swarm of users with the second swarm of users "because of the differences between the first, low definition file and the second, high definition file, the participants in the first swarm would not interact with those in the second swarm... That BitTorrent users have downloaded the same copyrighted work does not, therefore, evidence that they have acted together to obtain it."

B: *Hard Drive Productions, Inc., v. Does 1-188* (3:11-cv-10566-JCS)

Judge Joseph Spero further found that "under the BitTorrent Protocol, it is not necessary that each of the Does 1-188 participated in or contributed to the downloading of each other's copies of the work at issue – or even participated in or contributed to the downloading by any of the Does 1-188. Any 'pieces' of the work copied or uploaded by any individual Doe may have gone to any other Doe *or to any of the potentially thousands who participated in a given swarm.* The bare fact that a Doe clicked on a command to participate in the BitTorrent Protocol does not mean that they were part of the downloading by unknown hundreds or thousands of individuals across the country or across the world.

"Moreover, the court notes that the declaration submitted in this action, like the declaration in *Boy Racer*, appears to contradict the assertion that the Does named in this action are part of a single swarm.... [T]he exhibit attached to the complaint reflects that the activity of the different IP addresses occurred on different days and times over a two-week period.... Indeed, Plaintiff concedes that while the Doe Defendants may have participated in the same swarm, 'they may not have been physically present in the swarm on the exact same day and time'... As a result, the Court finds unpersuasive the allegation that the Does acted in concert. Therefore, the Court concludes that joinder of the Doe Defendants in this action Does not satisfy Rule 20(a)."

Here is a partial list of several other recent cases, all very similar in essential facts, where it was found that joinder was improperly applied:

- *Millennium TGA v. Does 1-21, Case No. 11-2258, N.D. Cal., Docket No. 8*
- *Boy Racer v. Does 2-52, Case No. 11-2834, N.D. Cal., Docket No. 12*
- *Diabolic Video Productions, Inc. v. Does 1-2099, No. 10-5865, N.D. Cal., Docket No. 16*

Because this improper joining of these Doe defendants into this one lawsuit raises serious questions of individual fairness and individual justice, the Court should sever the defendants and immediately dismiss the claims against Does 2-118.

2) Unreliability of IP Address Tracing.

The Plaintiff claims it has produced software that can reliably trace an IP address to a person. This statement is completely false. IP-tracing software has repeatedly been proven to be less than 100% reliable. A study conducted by Microsoft Research stated, "*We show that, even without built-in host identities, using IP addresses, anonymized user IDs, and their associated events, we can track a large percentage of host activities with high accuracy. Overall, 76% of the events in the application log can be attributed to hosts, and 92% of hosts can be tracked correctly. This result is consistent across many IP-address ranges [sic], suggesting tracking host-UP bindings is widely applicable.*" This report is freely available at the following URL:

http://research.microsoft.com/pubs/80964/sigcomm09.pdf.

This means that significant inaccuracies exist that allow Plaintiff to drag owners of IP addresses into this litigation that have absolutely nothing to do with the alleged wrongful activities, forcing them to incur wasteful time, money, and resources to defend themselves. Plaintiff alleges that the software referenced in their complaint is accurate in IP address tracing. It is difficult to believe that the Plaintiff has a more reliable software solution than Microsoft who spends millions of dollars in research to solve this problem.

There is also a separate issue here as well. In the case of someone using an unsecured wireless router, an outside party can access their internet connection. This party can surf the internet, send email, upload files, or download content. This unknown outside party would have the same IP address as anyone on the router itself. Therefore, there is no way to know, reliably and accurately, who the offending party was.

Many courts across the country have ruled against cases for these exact reasons. These cases are too numerous to list here. I ask that the Court support these rulings.

A search on Google.com reveals dozens of software solutions that allow users to "spoof" or impersonate false IP addresses via a proxy server (intermediary), which are designed to reroute traffic and obscure the source as well as the destination. This completely disproves the Plaintiff's claim (again) that they are able to pinpoint an individual based upon their IP address.

Common public examples of such software are:

http://www.torproject.org/
http://proxy.org/cgi_proxies.shtml
http://tech-faq.com/proxy

3) Unreliability of MAC Address Tracing.

For the subset of IP addresses that the Plaintiff has successfully tracked, one would need the Media Access Control address (MAC address) to find the material that the Does are accused of downloading. The MAC address would be a unique identifier to a device that downloaded the material. Any device with an internet connection has a unique MAC address. This would include routers, hubs, switches, wireless access points, desktops, laptops, smart phones, network attached storage, etc.

The issue here is that ISPs typically "bind" to one MAC address. This MAC address would be associated with what is directly connected to the ISP's modem, which generated the internet connection. In my particular network configuration, the MAC address that my ISP would report would be my wireless router. This device, unless equipped with a storage device, would have no files on it other than the routing software provided by the original equipment manufacturer (OEM). Once again, the Plaintiff has misrepresented their capabilities of tracing. In my network configuration, I have several devices connected to the router, including other potential known or unknown parties connecting through my wireless connection. Any of these could be associated with the complaint.

This proves that the Plaintiff's ability to 100% identify a *person* by their MAC address tracing software is completely false.

In addition, there are many solutions (and how-to guides) that are available free and online that allow an individual to impersonate of falsify MAC addresses (just like IP addresses). One such example can be found at http://hidemymacaddress.com/. This makes it extraordinarily difficult to pinpoint a specific device where the alleged offense occurred. The investigation would not know where to look to find the alleged download. This would be especially true if an unknown party connected to my wireless router and will not connect again. With this uncertainty, the Plaintiff's investigation would be unable to verify who and where the material was downloaded. As a result, the Plaintiff cannot pledge with certainty that I am the one who has allegedly downloaded their material.

4) Unreliability of Home Network Security

There is no way for the Plaintiff to prove that the Does in this complaint had a secured home network during the time of the alleged download. Even in the event that a Doe does have a secured home network, there are numerous ways to circumvent that security. One main example is WEP security, which I currently utilize, which is considered the lowest wireless security level, as well as the easiest to crack. One website claims that one has the ability to crack a WEP security key in 60 seconds, which can be found here: http://www.shawnhogan.com/2006/08/how-to-crack-128-bit-wireless-networks.html.

Another website shows every single step necessary as well as the appropriate items to buy and the tools to use to make it easier to attach someone's security: http://lifehacker.com/5305094/how-to-crack-a-wi+fi-networks-wep-password-with-backtrack.

5) Inability to Pinpoint a Person by IP Address

Unfortunately for the Plaintiff, the claim that their ability to pinpoint a person directly by an IP address is impossible, as stated previously. People commonly share computers and wireless networks within a household. These people are family members, friends and guests. Any of these people had the potential of downloading anything they wish. This could have included the alleged content as provided in the complaint.

In the event that someone breeched my wireless security, it would be someone who does not reside in my residence. I live in an area where there are many residences close by my own. I would have no way of knowing who intercepted my wireless signal and used it for their own purposes. Moreover, an unknown party could have been on a laptop in a car across the street accessing my wireless network. There would be no way of knowing. As a result, the Plaintiff has a very difficult job of identifying someone with any certainty. They should not be allowed to impose undue expense and burden on 118 people to disprove their case when the foundation of their allegations is so unreliable and superficial.

Therefore, I respectfully request this honorable court quash the subpoena requesting subscriber information relating to my IP address issued against the Internet Service Provider in the instant case, and suspend discovery pursuant to the local rules. I also respectfully request an order protecting my identity, substantially in the form of "The subpoena seeking information from ISP regarding John Doe (72.129.105.245) (identity protected) is hereby quashed."

Dated: September 16, 2011

Respectfully submitted,

John Doe

John Doe (72.129.105.245)

Pro se