IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC,

Plaintiff,

vs.

DOES 1-22,

Defendants.

_____/

CASE No. 5:12-cv-02088-MMB

MOTION TO QUASH OR MODIFY SUBPOENA

MOTION TO DISMISS AND/OR SEVER COMPLAINT AGAINST DEFENDANT JOHN DOE #1 AND QUASH SUBPOENA AGAINST SAME

I, John Doe #1, hereby sincerely and respectfully move the court for dismissal or severance of my case in the above captioned matter and motion to quash the subpoena served on my Internet Service Provider, Comcast Corporation.

I have taken no part in the acts alleged by the plaintiffs. I also have never received any notice of illegal downloading activity from Comcast in regards to my IP or my service address, which is standard procedure for Comcast in the event that they detect this kind of activity, or they receive a warning from the third party companies that produced the downloaded material. After receiving a letter from Comcast Corporation advising me that they had been subpoenaed to release my identity and contact information in this matter, I was shocked. I began to research Malibu Media, LLC, as well as Christopher Fiore. My internet research has revealed that the cases associated with Malibu Media, LLC and Christopher Fiore have the same results. When the subpoenaed information is turned over to the plaintiffs, the defendants, guilty or innocent,

receive demand letters. These letters typically demand from $2500 to $7500 and in some cases in excess of $13000 for settlement to avoid dealing with threatened lawsuits, and the subsequent telephone calls, which have been reported as persistent if not harassing. These are the reasons I am filing this motion. I respectfully request that I be allowed to make this motion anonymously without revealing my personally identifying information as to do otherwise would defeat the purpose of this motion.

I base this motion on four factors: (1) improper joinder, (2) the person using a device connected to the internet at any given time is not necessarily the individual to whom the involved Internet Protocol address (IP address) is registered, (3) even the MediaAccess Control (MAC) address will often indicate on the wireless router connected to the internet but cannot be relied upon to determine who accessed the internet at any particular time, and (4) the inability to identify who actually accessed the internet through given IP and MAC addresses introduces an unacceptable degree of uncertainty with regard to the identification of actual wrongdoers.

I . Improper Joinder

I am aware that the Court has found the joinder to be proper, but respectfully ask the Court to reconsider this ruling after reviewing the information I will be presenting.

To minimize court costs while suing or threatening to sue as many individuals as possible, Plaintiff's counsel, Christopher P. Fiore, is using improper joinders which has been typical in Malibu Media, LLC suits alleging copyright infringement through BitTorrent. Information retrieved from Justia Dockets and Filings (http://dockets.justia.comL) indicates that Mr. Fiore filed 5 lawsuits on behalf of Malibu Media, LLC in the Pennsylvania Eastern District Court on March 8, 2012. An additional 12 filings on behalf of Malibu Media, LLC were made

on April 19, 2012 and a further 9 on June 4, 2012. Altogether, these 26 Malibu Media, LLC lawsuits involve 443 defendants and have been assigned to 13 different judge s in the same district Court. The individual lawsuits have from 6 to 41 defendants each, averaging 17.

Thus far in 2012, Malibu Media LLC has filed more than 130 suits in California, Colorado, the District of Columbia, Florida, Maryland, New York, Pennsylvania, Texas and Virginia against numbered Does using similar tactics. These suits collectively name almost 2200 defendants, averaging almost 17 per case.

Federal courts have previously recognized this improperness of joinder. In a BitTorrent case nearly identical to this one, CP Productions, Inc. v. Does 1-300 case 1:201 Ocv06255, the court noted before dismissal:

> [I] f the 300 unnamed defendants have in fact infringed any copyrights (something that this court will assume to be the case, given the Complaint's allegations that so state), each of those infringements was separate and apart from the others. No predicate has been shown for thus combining 300 separate actions on the cheap - if CP had sued the 300 claimed infringers separately for their discrete infringements, the filing fees alone would have aggregated $105,000 rather than $350.

In the same vein, in the Southern District of New York, Judge Colleen McMahon wrote when dismissing all but one of the defendants (John Doe #1) in Digital Sins, Inc. vs. John Does J- 245 Caye J:JJ-cv-08J7()"cM, "They are dismissed because the plaintiff has not paid the filing fee that is statutorily required to bring these 244 separate lawsuits." In that case the underpayment exceeded $85,000.00.

Commenting on the same case, Judge Milton Shadur wrote:

> " This Court has received still another motion by a "Doe " defendant to quash a subpoena in this ill-considered lawsuit filed by CP Productions, Inc. ("CP") against no fewer than 300 unidentified "Doe " defendants - this one seeking the nullification of a February 11,2011 subpoena issued to Comcast Communications, LLC. This Court's February 24, 2011 memorandum opinion and order has already sounded the death knell for this action, which has abused the litigation system in more than one way. But because the aggrieved Doe defendants

continue to come out of the woodwork with motions to quash, indicating an unawareness of this Court's dismissal of this action, 1 CP' s counsel is ordered to appear in court on March 9, 2011 at 9:00 a.m. Counsel will be expected to discuss what steps should be taken to apprise all ofthe targeted "Doe " defendants that they will not be subject to any further trouble or expense as a result of this ill-fated (as well as ill-considered) lawsuit. "

In *VPR Internationale vs. Does 1-1017 case 2:20J1cv02068*, Judge Harold A. Baker wrote in denying a motion for expedited discovery:

"Plainly stated, the court is concerned that the expedited ex parte discovery is a fishing expedition by means of a perversion of the purpose of and intent of Fed. R. Civ. P. 23."

In the Northern District of California, these nearly identical BitTorrent cases have been severed for improper joinder:

Pacific Century International LTD v. Does 1-101 case :20J1cv02533 (severed does 2-101)

IO Group, Inc. v. Does 1-435 case 3:2010cv04382 (severed does 2-435)

Diabolic Video Productions, Inc v. Does 1-2099 case 5:2010cv05865 (severed Does 2-2099)

New Sensations, Inc v. Does 1-1768 case 5:2010cv05864 (severed Does 2-1768)

In yet another nearly identical BitTorrent case, filed in the Northern District of California, *Millennium TGA, Inc v. Does 1-21 case 3:20J1cv02258*, Judge Samuel Conti found the same joinder problems, and wrote in his order denying request for leave to take early discovery, "This Court does not issue fishing licenses;" Two other BitTorrent cases in the Northern District of California by the same plaintiff, Boy Racer, have also been severed for improper joinder:

Boy Racer, Inc v. Does 1-52 case 5:20J1cv02329 (severed Does 2-52)

Boy Racer, Inc v. Does 1-71 case 5:20J1cv01958 (severed Does 2-72)

In *Case 1:12-cv-00163-CMH-TRJ, Document 10*, United States Magistrate Judge Thomas Rawles Jones, Jr. of the United States District Court for the Eastern District of Virginia consolidated nine cases, eight in which Malibu Media, LLC was the plaintiff and recommended that:

"all but the first Doe defendant in each of these matters be severed, and that the plaintiffs then be permitted to serve discovery on these remaining defendants' internet service providers to learn their identities."

In the same document, the Judge cites precedence from two earlier cases arguing against joinder (p. 7, ibid): that "the allegation that defendants used the same protocol on different days and times was insufficient" and that "the span of time covering the activity made the argument for joinder "unpersuasive." The same logic applies to the present case. The complaint shows that the alleged infringements took place on the following dates:

January 3, 2012 (Doe #14), January 11, 2012 (Doe #6), January 15, 2012 (Doe #12), January 21, 2012 (Doe #2), January 22, 2012 (Doe #1), January 27, 2012 (Doe #8), February 8, 2012 (Doe #7), February 15, 2012 (Doe #15), February 18, 2012 (Doe #4), February 22, 2012 (Doe #11), March 2, 2012 (Doe #3), March 9, 2012 (Doe #10), March 12, 2012 (Doe #13), March 14, 2012 (Doe #5), and March 15, 2012 (Doe #9).

Note that the dates span more than two months and on no occasion were any two defendants alleged to be active on the same date.

2. The person using a device connected to the internet at any given time is not necessarily the individual to whom an implicated Internet Protocol IP address) is

registered.

There are many circumstances in which the person to whom an Internet Protocol address may be registered is not the only person able to access the internet through that address. These are discussed at length in a Declaration (*Case 2: 12-cv-02084-MMB Document 9*). A copy of this Declaration is attached at the end of this motion, after the Certificate of Service. The fact that the person to whom an IP address is registered may not be the only individual who can access the internet through that address, and the implications of this have been recognized previously by the courts. In *Case 2:II-cv-03995*, the Honorable Gary Brown noted that

> "it is no more likely that the subscriber to an IP address carried out a particular computer function -here the purported illegal downloading of a single pornographic film- than to say an individual who pays the telephone bill made a specific telephone call" [p. 6]

3. Even a valid Media Access Control (MAC) address will often indicate only the wireless router connected to the internet and cannot be relied upon to determine who accessed the internet at any particular time.

The identity of devices connected to the internet through an IP address is often limited to the first in a chain of devices. With the advent of the wireless router, often this will be the only device that can be identified. However, ownership of a wireless router, even a secured one, is not tantamount to being the only possible user of the device. Therefore, even the MAC address logged by the Internet Service Provider is of limited and possibly no value in determining who accessed the internet at a given moment or even what computer or other device was used to do so. This is discussed in more detail in the Declaration referenced in (2) above. This has explicitly been recognized in the courts by Judge Gary R. Brown who wrote in RE: BITTORRENT ADULT FILM COPYRIGHT INFRINGEMENT CASES (Case 2-11-cv-03995-DRH-GRB Document 39) that:

> Unless the wireless router has been appropriately secured (and in some cases even if it has been secured), neighbors or passersby could access the Internet using the IP address assigned to a particular subscriber and download the plaintiff's film. As one court noted:
>
> In order to allow multiple computers to access the internet under the same IP address, the cable modem may be connect to a router, or may itself function as a router, which serves as a gateway through which multiple computers could access the internet at the same time under the same IP address. The router could be a wireless device in which case, computers located within 300 feet of the wireless router signal could access the internet through the router and modem under the same IP address. The wireless router strength could be increased beyond 600 feet if additional devices are added. The only way to prevent sharing of the wireless router is to encrypt the signal and even then an individual can bypass the security using publicly available software. [pg. 7, citations absent in the original]

4. The inability to identify who actually accessed the internet through implicated IP and MAC addresses introduces an unacceptable degree or uncertainty with regard to the identification or actual wrongdoers.

If, as may often be the case, it is not possible to identify the device used to access the internet, much less the person operating the device, simply classifying all persons to whom implicated IP addresses are registered as offenders creates a significant possibility, even probability if repeated often enough, that a number of persons who have done no wrong will be served and possibly elect to settle claims out of court as an expedient. For some this may be a simple business decision: it will cost less to settle than to litigate; for others who lack the financial resources to mount an adequate defense, the "choice" is forced upon them. This creates the potential for a coercive and unjust settlement and this has also been recognized by the courts in various jurisdictions. The Honorable Gary R. Brown writing on *Case* 2: *ll-cv-03995* (document 39) when evaluating the potential for coerced settlements noted that:

> Many courts evaluating similar cases have shared this concern. *See, e.g., Pacific Century Int'l, Ltd* v. *Does* 1-37-F. Supp. 2d--, 2012 WL 26349, at *3 (N.D. IlL Mar. 30,2012) ("the subscribers, often embarrassed about the prospect of being named in a suit involving pornographic movies settle"); *Digital Sin, 2012* WL 263491, at 3 * ("This concern and its potential impact on social and economic relationships, could impel a defendant entirely innocent of the alleged conduct to enter into an extortionate settlement") *SBO Pictures,* 2011 WL 6002620, at *3 (defendants, whether guilty of copyright infringement or not would then have to decide whether to pay money to retain legal assistance that he or she illegally downloaded sexually explicit materials, or pay the money demanded. This creates great potential for a coercive and unjust 'settlement'"). [pg 18]

The Honorable Harold A. Baker noted when commenting on *VPR Internationale v. DOES 1-1017 (2:11-cv-02068-HAB -DGB # 15),* that:

> Orin Kerr, a professor at George Washington University Law School, noted that whether you're guilty or not, "you look like a suspect."3 Could expedited discovery be used to wrest quick settlements, even from people who have done nothing wrong? The embarrassment of public exposure might be too great, the legal system too daunting and expensive, for some to ask whether VPR has competent evidence to prove its case. In its order denying the motion for expedited discovery, the court noted that until at least one person is served, the court lacks personal jurisdiction over anyone. The court has no jurisdiction over any of the Does at this time; the imprimatur of this court will not be used to advance a "fishing expedition by means of a perversion of the purpose and intent" of class actions. Order, *die* 9. [pg 3]

Magistrate Judge Harold R. Loyd writing in regard to *"Hard Drive Productions v. Does 1-90, C/1-03825 HRL* stated:

> Here, plaintiff has failed to allege that its claims against the 90 Doe defendants arise from "a single transaction or a series of closely related transactions." Instead, plaintiff provides a list of all 90 Doe defendants, identified by IP addresses, and the date and time they each appeared in the swarm over a period of63 days. See Complaint, Exh. A. Plaintiff also alleges that each Doe defendant "entered the same exact BitTorrent swarm and "reproduced and distributed the Video to multiple third parties." Complaint 29. But, plaintiff's counsel admitted at the hearing that plaintiff could not truthfully allege that any of the Doe defendants actually transferred Ted pieces of the copyrighted work to or from one another. [pg 10, emphasis added]

In *Case 2:11-cv-03995* which addressed three cases *(Malibu Media, LLC v. John Does* 1-26, *CV 12-1147 (J..)) (GRB). lvlalibu Media, LLC v. John Does 1-1I,* C'V *12-1I50 (LDW) (GRB),* and *Patrick Collins, 1nc. v. John Does* 1-9, *CV 12-1154 (ADS) (GRB))*

U.S. Magistrate Judge, the Honorable Gary Brown in discussing these issues noted that:

> '" These developments cast doubt on plaintiff's assertions that "[t]he ISP to which each Defendant subscribes can correlate the Defendant's IP address to the Defendant's true identity." *See, e.g., Alalibu* 26, CompL At ~9, or that subscribers to the IP addresses listed were actually the individuals who carried out the complained of acts. *As* one judge observed: The Court is concerned about the possibility that many of the names and addresses produced in response to Plaintiff's 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 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 tum out to be a neighbor in an apartment building that uses shared IP addresses or a dormitory that uses shared wireless networks. The risk of false positives gives rise to the potential for coercing unjust settlements from innocent defendants such as individuals who want to avoid the embarrassment of having their names publicly associated with allegations of illegally downloading "My Little Panties # 2" [pgs. 7 -8, citations omitted in the original, emphasis original].

Judge Brown also observed that another judge had previously noted [citations omitted in the original]:

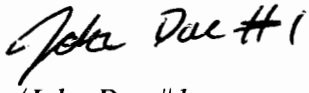
> the ISP subscriber to whom a certain IP address was assigned may not be the same person who used the Internet connection for illicit purposes... By defining Doe Defendants as ISP subscribers who were assigned certain IP addresses, instead of the actual Internet users who allegedly engaged in infringing activity, Plaintiff's sought-after discovery has the potential to draw numerous internet users into the litigation, placing a burden upon them that weighs against allowing the discovery as designed. [ibid, p. 8] Finally, also writing in case 2: *ll-cv-03995,* Judge Brown described the litigation practices in cases where pre-service discovery is the basis for identifying putative defendants as "abusive" and went on to state: Our federal court system provides litigants with some of the tiniest tools available to assist in resolving disputes; the courts should not, however, permit those tools to be used as a bludgeon. As one court advised Patrick Collins Inc. in an earlier case, "while the courts favor settlements, filing one mass action in order to identify hundreds of doe defendants through pre-service discovery and

facilitate mass settlement, is not what the joinder rules were established for." Patrick Collins, Inc. v. Does 1-3757,2011 U.S. Dist. LEXIS 128029, at *6-7 (N.D.Cal. Nov. 4, 2011).

from this matter and quash the subpoena for identifying and contact information served on Comcast Corporation for me, John Doe #1, only.

Dated: *7/2/2012*

Respectfully submitted,



s/John Doe #1
John Doe
Pro se

CERTIFICATE OF SERVICE

I, John Doe #1, hereby certify that on July 2, 2012, I forwarded a true and correct copy of Motion to Dismiss and/or Sever Complaint Against John Doe #1 and Quash Subpoena Against Same to Christopher P Fiore, Esquire, Fiore and Barber, LLC, 425 Main Street, Suite 200, Harleysville, PA 19438 by United States first class mail.

John Doe #1

s/John Doe #1
John Doe
Prose

THE FOLLOWING ATTACHMENT IS THE PREVIOUSLY MENTIONED DECLARATION FROM CASE 2:12-cv-02084-MMB

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC,

Plaintiff,

v.

JOHN DOES 1-14,

Defendants.

_____/

CASE No. 2:12-CV-02084

DECLARATION TO REFUTE INFORMATION PROVIDED BY PLAINTIFF'S COUNSEL, CHRISTOPHER FIORE, 14 MAY 2012 HEARING

I, an anonymous John Doe, do hereby declare:

1. I'm over 18 years of age and competent to make this declaration.
2. I have personal knowledge of the facts in this declaration and the information provided by Plaintiff's counsel, Christopher Fiore, on 14 May 12 (Document #6), during the motion hearing for cases 2:12-CV-02078, 2:12-CV-02084, and 2:12-CV-02088 (Malibu Media LLC is the Plaintiff for these cases), in support of Plaintiff's motion for leave to take discovery prior to Rule 26(f) conference.
3. I have also sent six previous declarations (October 2011 – January 2012) for copyright infringement cases for various courts: Eastern District of Virginia (Richmond Division), *3:11-cv-00531-JAG (Patrick Collins v. Does 1-58), 3:11-cv-00469-JAG (K-Beech v. Does 1-85),* District of Arizona, *2:11-cv-01602-GMS (Patrick Collins v. Does 1-54)*, the Northern District of Florida, *4:11-CV-00584 (Digital Sin, Inc., v. Does 1-145),* Northern District of Illinois, *1:11-CV-09064 (Pacific Century International v. Does 1-31),* and the District of Columbia, *1:12-cv-00048 (AF Holdings, LLC, v. Does 1-1058)*, refuting various Plaintiff

memorandums. Note: Four of the six declarations were accepted by the courts.

4. I'm filing this declaration anonymously, as I'm one of the 200,000+ John Doe defendants in the increasing number of copyright infringement cases filed throughout the U.S.[1] If I were to file this declaration under true name, I feel I would be singled out for vindictive prosecution by my Plaintiff and the network of copyright infringement lawyers that file these types of cases. The case I was under has been dismissed, but like many other Doe defendants, I'm waiting for the statute of limitation to expire. The declarations I have previously filed, and information I provide to Doe defendants on my Web site (*http://dietrolldie.com/*), have caused copyright infringement lawyers and Plaintiffs more work and the doubtless loss of settlement fees. To prevent identification, I will be mailing this declaration to the court and Plaintiff from a State other than my own.

5. Plaintiff will likely claim I have no standing to make this declaration, as I'm not one of the Doe defendants in this case. I believe I do have standing and valuable information concerning the information Mr. Fiore provided the court at the 14 May 12, hearing. As the hearing only sought clarification from Mr. Fiore, it is understandable the court would take his responses at face value. My standing is based on my direct knowledge of these types of cases and the operations of computer networks, to include small home/office networks, most (if not all) are what Plaintiff has listed as Doe defendants. I have gathered this knowledge first hand by working as a certified Information Technology Specialist, as a Doe defendant, and by running my Web site (*http://dietrolldie.com/*), dedicated to posting news and views concerning copyright infringement lawyers (AKA: Copyright Trolls) and John/Jane Does. While running my site, I have corresponded with many Doe defendants who like myself, are

---

[1] US News and World report, 2 Feb 12, Jason Koebler, *Porn Companies File Mass Piracy Lawsuits: Are You At Risk?*
http://www.usnews.com/news/articles/2012/02/02/porn-companies-file-mass-piracy-lawsuits-are-you-at-risk.

being abused by Plaintiffs and copyright infringement lawyers who follow this business model. Some of the Doe defendants I have interacted with have been pressured to settle with clients of Mr. Fiore for cases filed in the Eastern District of Pennsylvania.

6. I hope my declaration will aid the Court in understanding the questionable practices of Plaintiff, copyright infringement lawyers in general, and correcting the information Mr. Fiore presented the court during the 14 May 12, hearing. The anonymous nature of this declaration does not detract from its logic, truthfulness, and will only aid in the understanding of these technically complex types of cases. I thank the court for indulging this John Doe.

7. BitTorrent

BitTorrent is a computer program and protocol (system of rules) for sharing large files across the Internet. BitTorrent is part of a group of file sharing applications, known as peer-to-peer (P2P). BitTorrent is completely legal and only a tool in which the individual user decides how it is used. The company was founded in 2004 and their main office is located in San Francisco, CA. Details concerning BitTorrent can be found at www.bittorent.com. BitTorrent can and is used by personnel engaged in illegal file sharing, to include Plaintiff's movies. It is also used to legally distribute various files, to include software, music, ebooks, and movies. The BitTorrent Company and the various versions of its file sharing software are not hidden in some basement in Eastern Europe or Asia as Mr. Fiore suggests. This statement makes it seem that Mr. Fiore has very little knowledge on the software that plays a central part in these copyright infringement cases he is filing.

8. Wireless Networking

Mr. Fiore claims all the Doe defendants (public IP addresses) had to take active steps to install the BitTorrent software on their computers and was not an accidental matter.

Mr. Fiore omits to tell the court the public IP address Plaintiff's agents recorded does not necessarily correlate to the BitTorrent software being installed on any computer belonging to Doe defendants. The public IP address Plaintiff provided the court only correlates to the immediate location of the Internet service and who pays the Internet Service Provider (ISP). This is due to the fact that a majority of homes and small businesses today use a Wireless Firewall/Router (WFR) to share the Internet connection to systems at their location. The WFR allows multiple wired and wireless connections from computers (some possibility unauthorized); all using the same Public IP address Plaintiff has collected (Exhibit A). As the wireless signal of the WFR commonly extends outside the residence, it is not unusual for unauthorized systems to connect to it. Some ISP subscribers (Doe defendants) may have run their wireless Internet connection open (no password required), so anyone could have connected to it and downloaded Plaintiff's movie. Even if an ISP subscriber secures the wireless Internet connection with a password, there are various vulnerabilities that could be exploited to gain access to it.

Possible claims of negligence on the part of Doe defendants in not securing an Internet connection or by not monitoring what occurs on it are baseless. There is no legal duty or contractual obligation between the defendants and Plaintiff to require such action. On 30 Jan 12, Judge David Ezra, stated the following concerning negligence claims in copyright infringement case 1:11-cv-00262, Liberty Media Holdings, LLC, v. Hawaii members of swarm…,

> The Court concludes that the allegations in the FAC are not sufficient to state a claim for negligence for a couple reasons. First, nowhere in the FAC does Plaintiff assert any specific legal duty in connection with its negligence claim. Further, Plaintiff has not cited, nor has the Court found, any case law with analogous facts from which the Court could conclude that the Defendants owed Plaintiff a general duty to secure their internet connection. Second, even assuming

> Plaintiff had alleged a cognizable duty, the FAC fails to allege any facts demonstrating how Plaintiff breached that duty. Plaintiff's Memorandum in Opposition to the instant Motion highlights the purported risks associated with failing to password-protect one's wireless network. However, Plaintiff does not allege in the FAC that any of the individual Defendants failed to password-protect his/her wireless network or otherwise monitor the use of his/her computer by others. The bare assertion that they "failed to adequately secure their Internet access" is conclusory and unsupported by specific factual allegations regarding the individual Defendants. Therefore, it is not entitled to an assumption of truth for purposes of ruling on the instant Motion. (*1:11-cv-00262-DAE-RLP, Document #66, Order: (1) Granting in Part and Denying in Part Defendant Hatcher's Motion to Dismiss, (2) Granting Plaintiff's Leave to Amend, and (3)Vacating the Hearing, Page 13*)

The WFR provides each system connected to it an "internal" IP address that no one outside the home network will ever see (Exhibit A). The unauthorized use of a defendants Internet connection is sometimes unwittingly done by a neighbor, but has also been done by malicious third-parties wishing to avoid detection of illegal activity or to implicate a defendant in a crime. Due to the technical nature of the WFR, most users set-up the device and never touch it again unless there is a problem. Most users will never know their Internet connection was illegally used by third parties unless they receive some notification. One such common notification is the Digital Millennium Copyright Act (DMCA) take-down notice from a copyright content owner. Note: most pornography copyright content owners do not issue DMCA take-down notices to ISPs and their customers (Doe defendants). Due to the very limited network logging ability of most WFR, by the time the ISP notifies the subscriber of a legal action (such as this case), any WFR logs showing possible third-party users are long gone. If DMCA take-down notices were immediately issued to the ISPs and Doe defendants, there is a better chance of the WFR having relevant logs.

Two 2011 Federal court filings from defendants in a similar California copyright infringement case (*3:11-cv-02766-MEJ, Northern District of CA, Patrick Collins v. Does 1-*

2590, Documents 22 and 52), show how weak the Public IP address is in identifying the actual copyright infringers.

In document 22 (*3:11-cv-02766-MEJ*), Bobbie Thomas (ISP subscriber), Richmond, CA, tells the court she is a disabled female who lives with her adult daughter and several in-home care providers. The residence (location of the Public IP address) is a three-story building in which her daughter runs a child day care business for 12-hours a day. In the first floor common area, Mrs. Thomas' personal computer and Internet connection were open and available for any of the residents or anyone with access to use.

In document 52 (*3:11-cv-02766-MEJ*), Steve Buchanan (ISP subscriber), Phoenix, AZ, tells the court that unknown personnel were abusing his Internet connection and his ISP had to help him re-secure his WFR. Mr. Buchanan enlisted the help of his ISP after receiving notification from his ISP that copyright protected movies were being shared via his public IP address. Mr. Buchanan eventually secured his WFR and determined that unknown personnel had also illegally accessed his wife's computer and prevented it from connecting to his network.

The unauthorized use of a home WFR led to one Buffalo, NY, family to being investigated for allegedly downloading child pornography. On 7 March 2011, US Immigration and Customs (ICE) agents executed a search warrant for child pornography based only on the subscriber information (Public IP address) they received from the ISP. ICE later determined that a next-door neighbor had used the Internet connection via the WFR. [2]

In July 2011, Barry Ardolf, Minnesota, was convicted of hacking a neighbors (Matt and Bethany Kostolnik) WFR, trying to frame them with child pornography, sexual

---

[2] http://www.huffingtonpost.com/2011/04/24/unsecured-wifi-child-pornography-innocent_n_852996.html, ***Innocent Man Accused of Child Pornography After Neighbor Pirates His WiFi, 24 Apr11.***

harassment, and even sending threading emails to Vice President Joe Biden.[3] Mr. Ardolf used freely available software and manuals to hack the Wired Equivalent Privacy (WEP) protecting the Kostolnik's WFR. Due to the threatening emails sent to the Vice President, the US Secret Service contacted Mr. Kostolnik based on the email and Public IP address. Mr. Kostolnik was eventually cleared of these allegations after it was determined Mr. Ardolf hacked their WFR. Mr. Ardolf was eventually sentenced to 18 years in prison (*case 0:10-cr-00159-DWF-FLN, USDC, District of Minnesota*).[4]

Examples of why the registered IP subscriber did not illegally download/share the copyright protected movie are:

a. Home Wireless Internet access point run open (like at an airport or coffee bar) and abused by an unknown person.
b. Guest at the residence abusing the Internet connection without the owner knowing.
c. Neighbor connects (knowingly or unknowingly) to the network and the owner doesn't know of this activity.
d. IP address is part of a group residence (roommates), apartment building, or small home business where a user (not the ISP subscriber) downloaded/shared copyright protected movie.
e. Home system infected by a Trojan Horse malware program and controlled by unknown personnel.
f. Unknown person hacks the Wireless security settings of the WFR to abuse the owners Internet connection.[5]

Without additional investigative steps, innocent personnel are bound to be implicated in infringement activity and pressured to pay a settlement to make the threat of a federal law suit go away. One earlier court noted the problem with only using the Public IP address to identify the alleged infringer:

---

[3] *http://www.networkworld.com/news/2011/071311-wifi-hack.html*, "Depraved" Wi-Fi hacker gets 18 years in prison, *13 Jul 11*.
[4] *http://www.wired.com/images_blogs/threatlevel/2011/07/ardolffedssentencingmemo.pdf*, Government's Position With Respect to Sentencing, 14 Jul 11.
[5] *http://www.kb.cert.org/vuls/id/723755*, WiFi Protected Setup (WPS) PIN brute force vulnerability, Vulnerability Note VU# 723755, 27 Dec 11

> Comcast subscriber John Doe 1 could be an innocent parent whose internet access was abused by her minor child, while John Doe 2 might share a computer with a roommate who infringed Plaintiffs' works. John Does 3 through 203 could be thieves, just as Plaintiffs believe, inexcusably pilfering Plaintiffs' property and depriving them, and their artists, of the royalties they are rightly owed. . . . Wholesale litigation of these claims is inappropriate, at least with respect to a vast majority (if not all) of Defendants. *BMG Music v. Does 1-203, No. Civ.A. 04-650, 2004 WL 953888, at *1 (E.D. Pa. Apr. 2, 2004)* (severing lawsuit involving 203 defendants).

Without informing the court of these facts, it is irresponsible for Mr. Fiore to tell the court that ALL the defendants installed BitTorrent software and knowingly took part in the illegal download/sharing of a copyright protected movie just because Plaintiff recorded their public IP address.

9. Media Access Control (MAC) Address

The MAC address the ISPs have on record for Doe defendants is a type of serial number found on devices with a computer networking capability. Common networking enabled devices include computers, smart phones, video game systems, televisions, and DVD players. Many ISPs use the MAC address as a screening filter to limit access to their network to only the paying customers. Depending on the specific ISP, the MAC address recorded may be for the cable/DSL modem or the first network enabled device connected to the modem. If a Doe defendant only has one computer connected directly to the cable/DSL modem, then the ISP may record the MAC address for this device. As it is common today for personnel to first connect a WFR into the cable/DSL modem, the MAC address recorded by the ISP may be for this device. None of MAC addresses for the internal devices connected to the WFR (wired or wireless) are seen or recorded by the ISP or anyone else outside of the home network (Exhibit A). As previously stated, the logging ability of the WFR is very limited and the fact that Plaintiff waited so long to file this case, relevant logs are likely gone.

10. Determination of the Actual Infringer

Plaintiff has no intention of identifying the actual copyright infringers with this action. Plaintiff's goal is to obtain ISP subscriber information for the public IP addresses they recorded, issue settlement demands, and eventually dismiss the cases without naming or serving a single defendant. Plaintiff claims the public IP address shows the ISP subscriber is responsible for the infringement activity. As shown above, this logic is flawed and to truly determine the infringer, more investigative effort has to be accomplished. The history of copyright infringement law suits by pornography content owners shows the overwhelming majority of defendants are never named and served with a summons. On 24 Feb 2012, Prenda Law Inc., one of the main copyright infringement law firms in the U.S., stated the following.

> Although our records indicate that we have filed suits against individual copyright infringement defendants, our records indicate no defendants have been served in the below listed cases. (*AF Holdings LLC, v. Does 1-135, case 5:11-cv-03336-LHK (NDCA), Document 43 (Declaration of Charles Piehl), Exhibit A, section 9.*)

Note: the number of cases in the Prenda document was 118, with over 15,000 Doe defendants since 2010. Out of 15,000+ Doe defendants, none were named and served with a summons (as of 24 Feb 12). I'm confident that if asked to produce a similar document, Mr. Fiore's report would be very similar for the cases he has filed in the EDPA.

11. Order & Report & Recommendation, Case 2:11-cv-03995, Judge Gary Brown (EDNY)

The basis of the 14 May 12, hearing was to address concerns the court had with Plaintiff's cases, as raised by Judge Brown's 1 May 12, Order & Report & Recommendation (ORR), Case 2:11-cv-03995, Document 39, Eastern District of New York. It is shocking Mr. Fiore didn't know about this ORR, as it deals with his client directly and was seen as a major set-back to the current copyright infringement law suits in EDNY and highly relevant to all law firms pursuing

these cases.

The court's question to Mr. Fiore about placing all of these types of copyright infringement cases under one judge is a valid one. Mr. Fiore doesn't directly state they shouldn't be placed under one judge, but he infers it is likely his view. Mr. Fiore incorrectly tells the court that as these copyright infringement cases are all "different," they should not be consolidated under the same judge. The issue is not that all of the EDPA pornography copyright infringement law suits have different Plaintiffs, different movies, and different Doe defendants. The key issue is they are all the same type of pornography copyright infringement law suit. Here are the main reasons why the EDPA should consolidate them under one judge (or limited number).

- These cases can be highly technical and a good understanding of computers/networking and Internet file sharing is needed. Having to repeatedly educate judges new to this case type on the technical aspects is a waste of limited judicial resources.
- The consolidation will ensure a uniform response for Plaintiffs and Doe defendant motions and case management, independent of which court the case is assigned to.
- All of the complaints for these cases are for Copyright Infringement in accordance with Title 17, Section 101.
- All of the alleged infringed copyright protected content is adult pornography.
- All of the alleged copyright infringement occurred via Internet file sharing applications, primarily BitTorrent.
- All the Plaintiffs in these cases employ some sort of technical monitoring service to record the public IP address of alleged infringers.
- All cases deal with Doe defendants who are only identified by their public IP address.

- All Plaintiffs seek leave to serve third party subpoenas prior to a Rule 26(f) Conference. The third party is the ISP who has the contact information (name, address, telephone number, email) for the subscriber assigned the public IP address Plaintiff recorded.
- Many Doe defendants in these cases file motions to quash, dismiss, or sever, based on claims of improper joinder, improper jurisdiction, or lack of prima facie evidence.
- Once the contact information for the Doe defendants are obtained, Plaintiffs make settlement demands of thousands of dollars to make the fear of a law suit go away.
- For over 200,000 Doe defendants nation-wide since 2010, there have only been a handful of default judgments issued. Most Plaintiffs dismiss the cases against non-settling Doe defendants. The goal with these types of law suits is not to prevent copyright infringement, but to generate revenue on a repeatable basis.

In his ORR (case 2:11-cv-03995), Judge Brown correctly describer the litigation practices of these cases as "Abusive."

> Our federal court system provides litigants with some of the finest tools available to assist in resolving disputes; the courts should not, however, permit those tools to be used as a bludgeon. As one court advised Patrick Collins Inc. in an earlier case, "while the courts favor settlements, filing one mass action in order to identify hundreds of doe defendants through pre-service discovery and facilitate mass settlement, is not what the joinder rules were established for." *Patrick Collins, Inc. v. Does 1–3757*, 2011 U.S. Dist. LEXIS 128029, at *6–7 (N.D.Cal. Nov. 4, 2011).

After my personal information was released to my Plaintiff, I was repeatedly threatened with an individual law suit. I was told I was responsible and there was no defense. I was told that unless I settled, the case would drag on for a year or two, and it

would cost me thousands more dollars than settling. My Plaintiff eventually dismissed the case after keeping it open for more than a year. I was never named in any complaint and never received a summons, even after repeated calls and letters stating they were about to take such actions. On 1 December 2011, Judge Maria-Elena James, Northern District of California (*case # 3:11-cv-02766-MEJ, Patrick Collins v. Does 1-2590*), commented on this practice.

> Since granting Plaintiff's request, a check of the Court's docket disclosed that no defendant has appeared and no proof of service has been filed. Further, the Court is aware that this case is but one of the many "mass copyright" cases to hit the dockets of federal district courts across the country in recent months. Like in this case, after filing the suit, the plaintiff seeks discovery from ISPs who possess subscriber information associated with each IP address. With the subscriber information in hand, the court is told, the plaintiff can proceed to name the defendants in the conventional manner and serve each defendant, so that the case may proceed to disposition. This disposition might take the form of settlement, summary judgment, or if necessary, trial. In most, if not all, of these cases, if the plaintiff is permitted the requested discovery, none of the Doe defendants are subsequently named in the cases; instead, the plaintiff's counsel sends settlement demand letters and the defendants are subsequently dismissed either by the Court or voluntarily by the plaintiff.

12. Conclusion

The copyright infringement of protected works, such as Plaintiff's, is a problem and the owners have the right to seek redress for it. Plaintiff's misuse of the court in seeking redress stems from the weak prima fascia evidence collected (public IP address) coupled with abusive settlement practices. Plaintiffs commonly set the settlement fee for defendants at the point where it costs them more to fight than settle, regardless of guilt or innocence. The threat of possible financial ruin, family and friend embarrassment, a convenient settlement option, and non-disclosure agreement, make it easy for even innocent people to possibly accept paying the settlement fee. Plaintiff knows their evidence collections methods are not 100% effective at identifying the actual infringers. To admit this short coming risks the prof-

itability of this business model and future operations. The fact that a majority of Federal civil cases are settled before trial should not be the justification basis for allowing this activity to continue. Plaintiff and the growing number of copyright infringement lawyers are abusing the court for their financial gain. These cases and other like it in the EDPA (past, present, and future) will follow the standard course of action: (1) release of ISP subscriber information, (2) settlement demands made by Plaintiff, and (3) dismissal of the cases after settlements are collected from some defendants (Noting that no defendants will be named and served).

I thank the court for hearing this declaration.

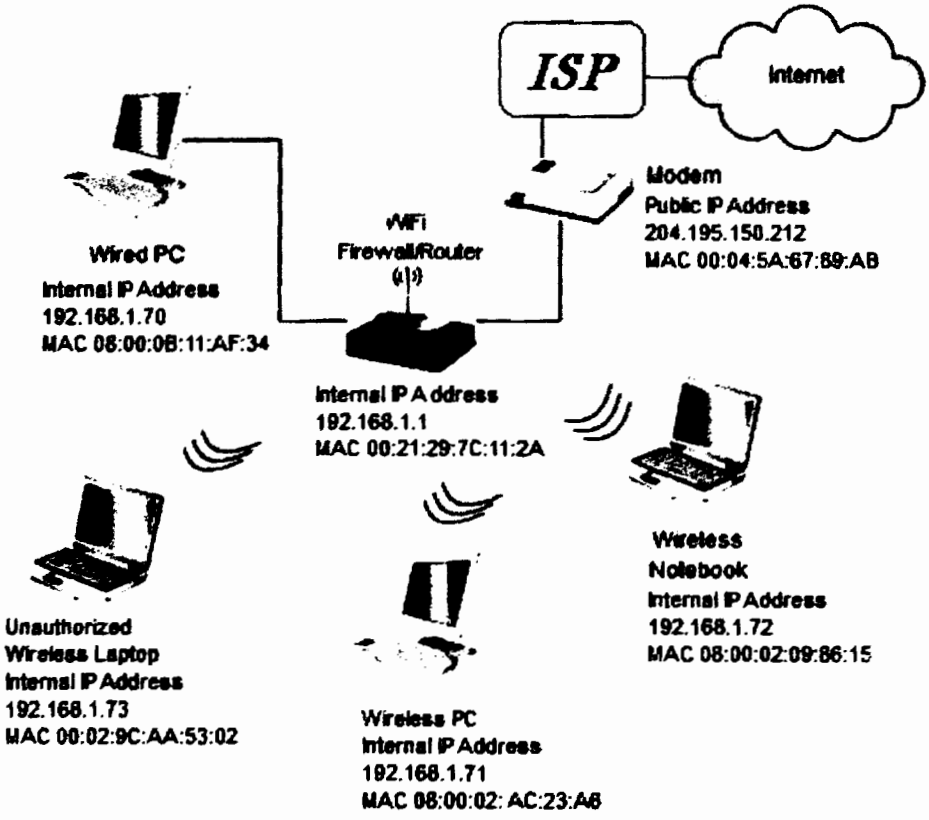
Dated: 5/31/2012

Respectfully submitted,

John Doe, AKA: DieTrollDie
Web site: *http://dietrolldie.com*
Doerayme2011@hotmail.com

EXHIBIT A (2:12-CV-02084)

Example of home network using a Wireless Firewall/Router



The following table is an example of a Dynamic Host Configuration Protocol (DHCP) host table maintained inside the Wireless Firewall Router. It shows the names, Internal IP address, MAC addresses, and IP address lease expiration time for systems that are connected to the network. Note: this example does not directly correspond to the network diagram above.

DHCP Active IP Table

DHCP Server IP Address: **192.168.1.1**

Refresh

Client Host Name	IP Address	MAC Address	Expires	Delete
SpureSPA	192.168.1.84	00:0E:08:CD:C9:96	20:01:49	☐
elephant-18adae	192.168.1.85	00:0C:76:88:C4:0A	08:49:53	☐
admin-lenoiby18	192.168.1.86	00:08:02:FE:88:22	23:43:47	☐
lucas-bu0n1jf3k	192.168.1.89	00:20:ED:33:70:F4	13:12:54	☐

Close

CERTIFICATE OF SERVICE

I hereby certify that on 5/31/2012, I served a copy of the foregoing document, via US Mail, on:

Fiore & Barber LLC
Attn. Christopher Fiore
425 Main Street, Ste 200
Harleysville, PA 19438

Dated: 5/31/2012

Respectfully submitted,

John Doe

John Doe, AKA: DieTrollDie
Web site: http://dietrolldie.com
Doerayme2011@hotmail.com