Thomas Freedman, OSB No. 080697
Email: thomas@prllaw.com
PEARL LAW LLC
522 SW 5th Ave. Ste. 1100
Portland, OR 97204
Phone: 503.295.6296
Counsel for Putative Defendant Jane Doe 19
(Identified by IP address 50.137.48.190)

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON - EUGENE DIVISION

ELF-MAN, LLC,
an Oregon corporation,

Plaintiff,

-against-

DOES 1-57.

Defendants.

Case No. 6:13-cv-00331-TC

PUTATIVE DEFENDANT JANE DOE 19's MOTION TO QUASH SUBPOENA

Oral Argument by Telephone Conference Requested (Local Rule 7-1(d)(3))

LR 7.1 CERTIFICATION

Pursuant to Local Rule 7-1, undersigned counsel conferred in good faith with plaintiff's counsel via telephone on April 10, 2013 to resolve the dispute and has been unable to do so. In addition, undersigned counsel conferred in good faith via telephone with the Comcast Legal Response Center on April 11, 2013 to resolve the dispute and has been unable to do so.

MOTION

Putative Defendant Jane Doe 19 (identified by IP address 50.137.48.190) ("Doe 19"), by and through undersigned counsel, hereby moves the Court to quash a subpoena directed to

Comcast Cable Legal Demand Center dated March 15, 2013 (the "Subpoena").[1] Defense counsel requests oral argument by telephone conference pursuant to Local Rule 7-1(d)(3).

In support of the motion, Doe 19 relies on the following memorandum of law:

Factual and Procedural Background

Plaintiff alleges that each of the 57 Doe defendants herein is liable for the infringement of plaintiff's alleged copyright in an obscure, straight-to-DVD motion picture entitled *Elf-Man* (*see generally* Cmpl.). Pursuant to an *ex parte* order, plaintiff has issued an unknown number of subpoenas seeking personal information about the putative Doe defendants, including a Rule 45 subpoena to Internet Service Provider ("ISP") Comcast seeking personal information concerning Doe 19 (the "Subpoena"). A copy of the Subpoena is annexed as Exhibit A to the Declaration of Doe 19, filed simultaneously herewith.

Plaintiff's counsel has filed at least nine similar federal lawsuits in Oregon, naming more than 1,000 defendants. See http://www.oregonlive.com/business/index.ssf/2013/04/estacada_woman_accused_of_ille.html. Upon learning the identity of a Doe defendant from his or her ISP, plaintiff's counsel's practice has been to send a threatening letter demanding $7,500.00 in two weeks or the individual will be publicly named in the lawsuit and face up to $150,000.00 in damages, plus costs, attorney fees and other consequences. *Id*.

A recent series of newspaper articles, including in the *Oregonian* and *Register Guard*, strongly criticize this practice, referring to it as "legal extortion":

> "Plaintiff lawyers build these cases by identifying Internet Protocol, or IP, addresses associated with movies downloaded to BitTorrent. They then subpoena service providers to hand over names of those customers and send letters such as

[1] Putative Defendant Jane Doe 19 does not concede that she is an actual defendant at this time, but merely a Comcast subscriber associated with the IP address 50.137.48.190 who will likely (and improperly) be named a defendant or receive a coercive demand letter from plaintiff in the event the Subpoena is not quashed. In any event, to the extent necessary, Doe 19 reserves all defenses, including as to jurisdiction and venue, in the event she is named a defendant herein.

> the one Orlando received [demanding $7,500 in two weeks or face a $150,000 judgment in federal court].
>
> Consumer and copyright lawyers criticize the strategy because, they contend, it's meant to scare consumers into costly settlements to avoid the far greater cost of litigation. They liken it to a reverse class-action in which hundreds of defendants are named. That allows plaintiffs [to] pay a single filing fee -- typically a few hundred dollars -- as opposed to filing and paying for hundreds of individual suits.
>
> The lawsuits, they say, also leave a ripple of more damaging effects -- defendants being identified through a less-than-reliable mechanism, consumer data being released to third parties and an overwhelmed federal court system.
>
> 'It's terrifying, it's legal extortion,' said Orlando, who'd never heard of BitTorrent before the letter.
>
> 'I won in the 'Bad Lottery,'' she said, 'I didn't do anything, but now I have to get a lawyer and fight this.'"

Id. (emphasis added).

Just like the 64-year old woman profiled in the *Oregonian* article, Doe 19 did not copy, publish, upload, download, share, stream, distribute, sell, record, access or view *Elf-Man* via BitTorrent (or any other source) at any point in time (Declaration of Doe 19, ¶ 1). In fact, Doe 19 was not even aware of *Elf-Man* until she received notice of the Subpoena from Comcast (*id*. ¶ 2). Moreover, Doe 19 has never used BitTorrent, and has no personal knowledge as to who allegedly used BitTorrent to access *Elf-Man* in connection with IP address 50.137.48.190 (*id*. ¶¶ 3-4).

Nonetheless, Doe 19 is now unfairly forced to incur extensive litigation costs, and is being subjected to unnecessary and undue stress, burden and fear even though she did not engage in any illegal activity.

Argument

I. The Subpoena Should Be Quashed Because the Information Sought Is Not Relevant

"The foremost fundamental principle regarding subpoenaed discovery is that a subpoena *duces tecum* to obtain materials in advance of trial should be issued only when the party seeking the materials can show that the materials are evidentiary and relevant." *Straily v. UBS Fin. Servs., Inc.*, 2008 WL 5378148, at *1 (D. Col. Dec. 23, 2008); 81 Am. Jur. 2d Witnesses § 20. A subpoena may be quashed when a subpoena seeks irrelevant information. *See Auto-Owners Ins. Co. v. Southeast Floating Docks, Inc.*, 231 F.R.D. 426, 429 (M.D. Fla. 2005); *Concord Boat Corp. v. Brunswick Corp.*, 169 F.R.D. 44, 49 (S.D.N.Y. 1996); Fed. R. Civ. P. 26(b).

The term "relevant" as used in Rule 26 and implied in Rule 45 is broad, but not exhaustive. While matters which may aid a party in the preparation or presentation of its case are relevant, matters without bearing either as direct evidence or as leads to evidence are not within the scope of inquiry. *See Lewis v. United Air Lines Transp. Corp.*, 27 F. Supp. 946 (D. Conn. 1939). As the Subpoena here was issued prior to a Rule 26(f) conference, the relevancy of the discovery sought should be even more narrowly tailored to that information which is necessary to definitely and immediately allow plaintiff to proceed with this lawsuit.

The discovery requested through the Subpoena is based on the faulty assumption that the Internet subscribers identified in Exhibit A to the Complaint are the individuals who actually infringed plaintiff's alleged copyright. The only individual that can be identified through an IP address is an ISP subscriber. Many courts have recognized that "the ISP subscribers to whom a certain IP address was assigned may not be the same person who used the Internet connection for illicit purposes." *SBO Pictures, Inc. v. Does 1-3036*, 2011 WL 6002620, at *3 (N.D. Cal. Nov. 30, 2011); *see also, e.g., In re: Ingenuity 13 LLC*, No. 2:11-mc-0084-JAM-DAD, Order [Doc. No. 24], at

*10 (E.D. Cal. Mar. 21, 2012) ("the identities of the subscribers associated with the identified IP addresses … would not reveal who actually downloaded petitioner's work, since the subscriber's internet connection could have been used by another person at the subscriber's location, or by an unknown party who obtained access to the subscriber's internet connection without authorization"); *Hard Drive Prods., Inc. v. Does 1-130*, 2011 WL 553960, at *2 (N.D. Cal., Nov. 16, 2011) ("Plaintiff concedes, in some cases the Subscriber and the Doe Defendant will not be the same individual"); *Pac. Century Int'l Ltd. v. Does 1-101*, 2011 WL 5117424, at *2 (N.D. Cal. Oct. 27, 2011).

An IP address provides only the location at which one of any number of computer devices may be deployed, especially when used with a wireless router.[2] The United States District Court for the Eastern District of New York noted that:

> If you only connect one computer to the Internet, that computer can use the address from your ISP. Many homes today, though, use routers to share a single Internet connection between multiple computers. Wireless routers have become especially popular in recent years, avoiding the need to run network cables between rooms. If you use a router to share an Internet connection, the router gets the IP address issued directly from the ISP. Then, it creates and manages a subnet for all the computers connected to that router.

In re: BitTorrent Adult Film Copyright Infringement Cases, 2012 WL 1570765, at *3 (E.D.N.Y. May 1, 2012) (quoting "What is an IP address?" available at http://computer.howstuffworks.com/internet/basics/question5492.htm). Thus, it is even less likely that an ISP subscriber (*e.g.*, Doe 19) carried out a particular computer function than an individual who pays a home telephone bill made a specific call. It is possible that any co-tenant living in that household, or visitor of that household, could have performed the complained of infringement. Unless the wireless router had been appropriately secured (and that security had not been compromised),

[2] One study has shown that 61% of all U.S. homes now have wireless access to the Internet. *See* Lardinois, F. "Study: 61% of US Households Now Have WiFi," available at http://techcrunch.com, 4/5/2012.

neighbors or a passersby could assess the Internet using the IP address assigned to a particular subscriber and download the movie in question. Illustrating this fact, the court in *VPR Int'l v. Does 1-1017*, 2:11-cv-02068-HAB-DGB (C.D. Ill. Apr. 29, 2011) cited an instance involving a raid by federal agents on a home that was linked to downloaded child pornography: The identity and location of the subscriber were provided by the ISP. The desktop computer, iPhones, and iPads of the homeowner and his wife were seized in the raid. Federal agents returned the equipment after determining that no one at the home had downloaded the illegal material. Agents eventually traced the downloads to a neighbor who had used multiple ISP subscribers' Wi-Fi connections (including a secure connection form the State University of New York). *Id*. at 2 (citing Carolyn Thompson, Bizarre Pornography Raid Underscores Wi-Fi Privacy Risks (April 25, 2011), http://www.msnbc.msn.com/id/42740201 /ns/technology_and_science-wireless/).

These circumstances create serious doubt as to plaintiff's claim that the expedited discovery sought will produce information sufficient to identify the individuals who actually infringed upon plaintiff's alleged copyright. 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 the individuals who actually downloaded or shared copyrighted material."

Digital Sin, Inc. v. Does 1-176, --F.R.D.--, 2012 WL 263491, at *3 (S.D.N.Y. Jan. 30, 2012) (emphasis added); *see also SBO Pictures*, 2011 WL 6002620, at *3. In a denying expedited discovery in a similar case, the Eastern District of California noted:

> "Although the revised Hansmeier declaration clarifies that he observed the co-conspirators' IP addresses engaged in the same downloading and uploading as John Doe, the declaration still does not establish that none of the internet subscribers whose information plaintiff seeks to obtain are innocent internet users. The concern remains that potentially non-offending users' information is

> being sought.… Because plaintiff seeks information about the '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 innocent internet users into the litigation, placing a burden upon them that weighs against allowing the discovery as designed."

First Time Videos, LLC v. Doe, 2012 WL 423714, at *5(E.D. Cal. Dec. 30, 2011) (emphasis added) (quoting *Hard Drive Prods*., 2011 WL 5573960, at *2).

Further, studies have shown that the type of tracking software used by investigators, such as IPP, International, to identify BitTorrent users often produces a large number of false positive IP hits. One study performed by the Department of Computer Science and Engineering at the University of Washington determined that "copyright holders utilize inconclusive methods for identifying infringing BitTorrent users. [The Researchers] were able to generate hundreds of DMCA takedown notices for machines under [their] control at the University of Washington that were not downloading or sharing any content." Michael Piatek et al., *Challenges and Directions for Monitoring P2P File Sharing Networks or Why My Printer Received a DMCA Takedown Notice*, 3rd USENIX Workshop on Hot Topics in Security 2008, (July 29, 2008) http://www.usenix.org/event/hotsec08/tech/full_papers/piatek/piatek.pdf. Specifically, the article concludes:

> "[W]e find that it is possible for a malicious user (or buggy software) to implicate (frame) seemingly any network endpoint in the sharing of copyrighted materials. We have applied these techniques to frame networked printers, a wireless (non-NAT) access point, and an innocent desktop computer, all of which have since received DMCA takedown notices but none of which actually participated in any P2P networks."

Id.

Accordingly, the information sought by plaintiff regarding the identity of Doe 19 is irrelevant to this lawsuit based on the inherent inaccuracy of the tracking software and the fact that many individuals will often access the Internet through the same ISP account. More

specifically, Doe 19 has submitted a sworn declaration stating that she did not copy, publish, upload, download, share, stream, distribute, sell, record, access or view *Elf-Man* via BitTorrent (or any other source), was not aware of *Elf-Man* until she received notice of the Subpoena from Comcast, has never used BitTorrent, and has no personal knowledge as to who allegedly used BitTorrent to access *Elf-Man* in connection with IP address 50.137.48.190 (*see* Declaration of Doe 19). The foregoing is a more than sufficient basis to quash the Subpoena.

II. The Subpoena Should Be Quashed Because It Seeks Confidential Information

Additionally, the Subpoena seeks confidential personally-identifying information that Comcast has on file about its subscriber Jane Doe 19.[3] Section 551 of the Cable Communications Act of 1984 requires that ISPs notify their subscribers before disclosing any personally identifiable information. 47 U.S.C. § 551(c)(2); *Doe v. Cahill*, 884 A.2d 451, 455 n.4 (D. Del. 2005); H.R. Rep. 98-934, at *77 ("Subsection (c) limits the disclosure of personally identifiable information collected by a cable operator to those situations … required by court order, provided that the subscriber has been notified of the disclosure . . ."). Congress established this requirement because subscribers have a privacy interest in their personally identifying information on record with their ISPs. H.R. Rep. 98-934, at *79 ("The Congress is recognizing a right of privacy in personally identifiable information collected and held by a cable company…").

Accordingly, Doe 19 holds a congressionally-recognized privacy interest in the confidential information sought by plaintiff regarding her identity, and the Subpoena should be quashed on this basis as well.

[3] Many ISPs, including Comcast, qualify as a "cable operator's" as defined by 47 U.S.C. § 522(5).

III. The Subpoena Should Be Quashed Due to "Undue Burden" Arising from Plaintiff's Bad Faith Litigation Tactics

As set forth *supra* and in a recent series of news articles, plaintiff is utilizing unreliable information to extort money from thousands of individuals, many of whom – like Doe 19 -- did not engage in copyright infringement or any illegal activity whatsoever. Due to the high cost of litigation and the fear and embarrassment of being publicly named in a federal lawsuit (particularly one bearing more than a passing resemblance to downloading pornography), many innocent individuals are coerced into paying money when they have done nothing wrong:

> "BitTorrent-related copyright infringement cases began popping up in earnest two years ago in the Midwest and California. Early on, most had accused defendants of downloading porn. In those cases, defendants received notice that if they didn't pay around $2,000, then they'd be named in federal cases.
>
> 'People understood their name would be out there in a public record that's probably going to stay on Google for a long, long time whether they'd done anything or not,' said Kenan Farrell, a copyright lawyer based in Indianapolis who tracks such cases there and in Oregon. 'There were very descriptive titles that people didn't want their names associated with, and they'd pay the $2,000.'"
>
> As firms found success in reaching settlements, the number of cases grew and spread geographically and across movie titles."

http://projects.registerguard.com/apf/tech/estacada-woman-among-371-oregonians-accused-of-illegally-downloading-steven-seagal-movie/

As set forth in the accompanying Declaration, Doe 19 did nothing illegal or actionable, has never used BitTorrent, and had never even heard of *Elf-Man* until Comcast sent her the Subpoena. Nonetheless, Doe 19 is now forced to incur unnecessary litigation costs, expense, burden, stress and disruption to her life. If the Subpoena is not quashed, Doe 19 will undoubtedly receive a coercive demand from plaintiff for $7,500.00, adding more undue stress and expense to her life, and be publicly named in the lawsuit if not paid in two weeks.

Accordingly, the Subpoena should be quashed on this basis as well. *See generally* FRCP 45(c)(3)(A)(iv) (the Court "must" quash a subpoena that "subjects a person to undue burden").

Conclusion

For the foregoing reasons, Putative Defendant Jane Doe 19 (identified by IP address 50.137.48.190) respectfully requests that the Court issue on Order (i) quashing the Subpoena and (ii) granting such other and further relief as the Court may deem just, equitable and proper.

Dated: April 11, 2013

Respectfully submitted,

PEARL LAW LLC

By: /s/ *Thomas Freedman*
Thomas Freedman, OSB No. 080697
Attorney for Putative Defendant Jane Doe 19 (Identified by IP address 50.137.48.190)