

EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

THIRD DEGREE FILMS, INC.
20525 Nordhoff Street, Suite 25
Chatsworth CA 91311,

Plaintiff,

v.

DOES 1-152,

Defendants.

CA 1:11-CV-01833-BAH

DECLARATION OF STEPHEN HENDRICKS

My name is Stephen Walker Hendricks. I am an Advanced Systems Representative Tier 1 and Tier 2 (Tier 2 is obsolete but still my title) at Comcast Cablevision based in Whitmarsh, Maryland. I have been a micro computer builder, designer and support technician since 1980 having been employed also at Heath Zenith Computers in Towson, MD from 1986 to 1989 as a sales agent who also custom built, and maintained systems for government, business, and individual clients. In my job capacities it was my responsibility to assist clients in all manners of computer operations, including helping using to protect their computers from threats which included viruses, malicious software, hardware vulnerability as well as human threats.

I have been provided the Complaint and its exhibits in the case of *Third Degree Films, Inc. v. Does 1-152*, Case No: 1:11-cv-01833-BAH.

The Declaration of Jon Nicolini, Exhibit B to the Complaint, contains misleading and erroneous statements that must be corrected.

1. It is impossible for Comcast to determine what devices attained the IP addresses

attributed in Exhibit A to John Does 116 and 117. IP addresses are dynamically assigned using the Dynamic Host Configuration Program (DHCP) protocol. The use of dynamically assigned IP addresses means that any device that is connected to a Comcast Cable modem can have different IP addresses based on several different events. An IP address can be used by several different devices simultaneously on the local network (referred to as a subnet) with the use of malicious programming techniques which can obscure the origin of an actual computer's connection. A subnet may have a few IP addresses in use, or hundreds of IP addresses. An ISP connects to the Internet through a direct connection.

2. The main computers which establish this connection are in an office called the Head End. The computers which connect the end user's computer (or other device) to the Internet are referred to as the Head End Computers. The Head End Computers communicate with devices that are attached to its fiber optic and coaxial cable systems using a standard referred to as Data Over Cable Service Interface Specification (DOCSIS). DOCSIS devices include modems and cable television set top boxes, televisions, and other devices. These devices also connect to the Head End using Ethernet data protocol and appear to the local network as computer devices. Television, cable boxes, disc players, and other devices now commonly used in a home can all communicate using IP protocol.
3. The only criterion that a computer Ethernet device needs to establish a connection to a DOCSIS cable modem is that it must use a connection protocol (in ISPs like Comcast the protocol is DHCP) and that it must provide to the modem a hardware

address called a MAC address. A modem can provide a connection to the Internet which will give the device connected to the Internet an IP address. The ISP however, cannot determine any of the following:

- a. Whether the device using the Internet connection is a computer, mobile device, tablet, router, etc.
 - b. The precise location of the device, since the modem can be anywhere on a subnet
 - c. How many devices may be using a particular IP address to access the Internet
 - d. If the MAC address is a true MAC address representing the Ethernet device or one that is spoofed (copied and reused) by some other device (such as an Ethernet connection on a Linux computer system, or a router).
4. A specified IP address cannot be assumed to belong to any particular device since the hardware address of a device can be spoofed.
 5. It is not possible to say what devices were connected to Ms. Zwarycz's Comcast Internet connection, by whom they were being used, and where the devices were physically located at the time they being used (i.e., inside the house of Bailey Zwarycz, in a neighboring house, or in a vehicle parked outside the Zwarycz residence or in a nearby structure which has access by cable to the same subnet).
 6. In fact, it is impossible for anyone to determine what device negotiated the IP addresses attributed in Exhibit A to John Does 116 and 117.
 7. Knowing an IP address that was being provided to a cable modem connection

does not identify the device that is connected through that modem. Even if the copyrighted material in question was being delivered over the Internet through that IP address there is no way to know or prove where it originated or that the owner of the Internet connection with that IP address, if she owns a computer, ever hosted or was the source of said material. The material may have come from:

- a. Any device connected to the local subnet accessing the Internet through Ms. Zwarycz's Internet connection.
 - b. An external wireless connection.
 - c. An external relay through a remote control virus.
 - d. A smart phone, tablet, laptop, or even surreptitious access of the subscriber's computer gained by a computer hacker without Ms. Zwarycz's knowledge.
8. For the reasons stated above, it is false and baseless for the Nicolini Declaration to say that by knowing the IP addresses of John Doe 116 and 117 they could determine whether a computer had been used and if so, which computer. (See Jon Nicolini Declaration, Complaint Exh. B, Paragraphs 18-21.)
9. Even if an unknown person downloaded Plaintiff's film using the IP address Comcast associates with Ms. Zwarycz, that person could have been using a computer outside of the house of Ms. Zwarycz without her awareness, knowledge, or consent.

10. The primary upshot of the foregoing information for this case is that there is no way that Plaintiff could make a good faith allegation in its complaint that John Does 116 and 117 -- namely, Bailey Zwarycz,-- willfully and intentionally downloaded, copied, and distributed Plaintiff's film. (See Jon Nicolini Declaration, Exhibit B to Complaint, Paragraphs 18-21.)

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on January 29, 2012.


Stephen Walker Hendricks

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Third Degree Films, Inc.,

Plaintiff,

v.

Does 1 - 152,

Defendants.

DECLARATION OF
SENSEI ENTERPRISES, INC.

Case No: 1:11-CV-01833-BAH
Judge Beryl Howell

I, John W. Simek, declare as follows:

1. I am the Vice President of Sensei Enterprises, Inc. and have been so employed as such since January of 1997.
2. Sensei Enterprises is an information technology, information security and computer forensic company located at 3975 University Drive, Suite 225, Fairfax, VA 22030.
3. Sensei Enterprises has been retained to review documents and devices in connection with the matter of *Third Degree Films, Inc. v. Does 1-152*, specifically the following:
 - a. The Complaint and its Verification by Mike Meier, an attorney located at 4000 Legato Road, Suite 1100, Fairfax VA 22033- executed under the provisions of 28 USC Section 1746.
 - b. A Declaration filed in this action and prepared and executed by Jon Nicolini, Vice-President of Technology for Copyright Enforcement Group, LLC, of Beverly Hills California, executed under the penalty of perjury and stated to be of his personal knowledge.

- c. The Declaration of Bailey Zwarycz.
 - d. The laptop computer owned by the person identified in the Complaint as John Doe 116 and 117.
4. I disagree with numerous factual recitations and the conclusions drawn from those recitations by Messrs, Meier and Nicolini as set forth in the Complaint and the Declaration of Mr. Nicolini. The disagreements and the basis for the disagreements are as follows:
- a. The Complaint asserts, and Messrs, Meier and Nicolini endorse the assertions as factually accurate and truthful, that once the Plaintiff is provided the subscriber identity from the Internet Service Provider (ISP) as determined from the Internet Protocol (IP) address, that they will have learned the actual identity of the person or persons alleged to have willfully and intentionally downloaded the copyright protected film, otherwise known as "All About Kagney Linn Carter," an admitted pornography film. The IP addresses are identified in Exhibit A of the Complaint. Messrs, Meier and Nicolini misrepresent the conclusions as fact when only the IP address is known. The public IP addresses as identified in Exhibit A only represent the last identifiable hardware device that is connected to the Internet, through which the Plaintiff's copyrighted material may have passed on its way to a destination or destinations unknown.
 - b. The two IP addresses listed for John Doe 116 and John Doe 117 are associated with the same single physical device associated to a single subscriber. John Doe 116 and John Doe 117 are the same person, for which two unique dynamic IP addresses were assigned by the John Doe's Internet Service Provider.

- c. John Doe 116 and John Doe 117 shall hereinafter be referred to in the singular as "this John Doe."
- d. The device assigned the two IP addresses is passed through a cable modem, which is used to connect subscriber equipment to the ISP's network. The cable modem converts the signal of the ISP network to a format that is compatible with other network attached devices of the subscriber. This may include such items as a single computer, network switch or router. The cable modem itself does not record or store the transmitted information, but is merely a pass-through device changing one signal type to another for use by digital devices at each end. In no sense are they capable of downloading and storing the Plaintiff's protected material or applying any software to that signal to act as a "seed" or a "swarm" as described by the Complaint and the declarations of Meier and Nicolini.
- e. It is well known that the majority of users accessing the Internet via a broadband (e.g. cable modem, DSL, etc.) connection do so by using a router, which is a device that attaches to the cable modem or similar equipment and allows multiple users to access the Internet simultaneously through a single connection. Routers, like cable modems, are not in and of themselves capable of downloading, storing, recording, or manipulating data such as the Plaintiff's protected material. The presence of a router connected to the cable modem obtains the IP address assigned by the ISP and appears as if it is a single computer to the ISP.
- f. This John Doe's Internet service provider was Comcast and the cable modem used to connect this John Doe's computer to the Internet was also provided by Comcast, which maintained a record of the modem's Media Access Control

(MAC) address associated with it. The MAC address can be thought of as a hardware serial number for the device.

- g. This John Doe had acquired a wireless router independently of Comcast and the presence or absence of a router attached to her cable modem was not known or knowable to Comcast. Comcast only knows that *some* device is attached and presents itself as having a specific IP address.
- h. Routers may be "password protected" so that they theoretically can only be accessed by users who have knowledge of the correct password. In addition, the wireless "cloud" can also be password protected to prevent unauthorized access.
- i. Router owners, such as this John Doe, may grant as many people as they choose to access the Internet through their router [up to certain finite limits not relevant here].
- j. This John Doe can elect to use a wireless router which is not protected by a password, thus enabling anyone within the wireless signal range of the router to access the Internet through this device.
- k. Even if the wireless "cloud" was password protected there are several commercially available (and free) programs able to determine the wireless password and circumvent it.
- l. So long as the last identifiable device in the chain of distribution is a cable modem (known via MAC address), to which a wireless router may be attached, the ultimate user who accessed the Internet and downloaded some or all of the Plaintiff's protected material and used peer-to-peer network software to acquire,

assemble and redistribute its protected material may be unknown and indeterminate.

- m. Absent special software or hardware acquired for that purpose, knowing how many users may be accessing the Internet simultaneously through the same wireless router is not apparent to any person or persons utilizing the wireless router.
- n. I have been advised that this John Doe is a student at Virginia Polytechnic University (Virginia Tech) who attached an un-password-protected wireless router, which she obtained commercially, to her Comcast provided cable modem. At the time she did so she was unaware that the wireless "cloud" was not protected by a password and even unaware that the wireless "cloud" could be secured via a password.
- o. I have been advised that this John Doe accessed the Internet through the use of a laptop computer which connected wirelessly to her router. She has a vague memory of occasions when others who visited her in her quarters may have accessed the Internet wirelessly through her router. She was completely unaware that others outside her dwelling place might have access to the Internet through her router with or without her permission or knowledge.
- p. On the 2nd day of December, 2011, at the request of counsel, Sensei took delivery of her laptop computer, forensically acquired her entire hard drive and thereafter returned the laptop to her. We then conducted an examination of the contents of that hard drive, using professionally accepted techniques and tools, looking for any indication that at any time the laptop had downloaded, stored or manipulated

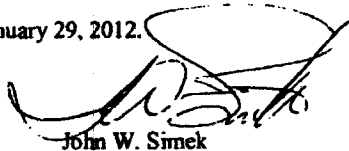
any portion or all of the Plaintiff's protected material, or had on its hard drive any software capable of participating in a peer-to-peer network, specifically for any part or all of a programs capable of participating in a BitTorrent network.

- q. The techniques and tools used would have uncovered any indicia of the downloading, storing or manipulation of the Plaintiff's protected material currently on the computer system, and even if that material had once been present but was subsequently deleted or uninstalled, remnant data or artifacts of such data would most likely still be present.
- r. The same professionally accepted techniques and tools were used to search for any indicia of the past or present use of peer-to-peer software or the BitTorrent network. No evidence was discovered of such usage or presence of software to facilitate usage.
- s. It is my professional judgment that at no time in the past or in the present has the hard drive of this John Doe's computer contained any part of the Plaintiff's movie "All About Kagney Linn Karter" or any part of peer-to-peer software or BitTorrent network access. I hold this opinion with a high degree of confidence, that is, to a reasonable degree of scientific certainty.

- 5. In the Meier verified Complaint and the Declaration of Jon Nicolini they further contend that they were able to determine that all of the John Does, including John Does 116 and 117 were within the jurisdiction of this court, contending they used "geo-location technology..." to attempt to "ensure that the IP Addresses are likely within the geographic location of the Court."

- a. Mr. Meier specifically asserts that he “personally spot checked the purported location of the alleged infringers...” using “the IP locator at <http://www.ipligence.com>.”
 - b. According to the Declaration of this John Doe, the location of the wireless router connect to the Comcast cable modem represented by those two listed IP addresses for John Doe 116 and 117 is and always has been in Blacksburg, Virginia.
 - c. When I used the website (<http://www.ipligence.com>) specified by Mr. Meier to determine the probable location of the IP addresses stated for John Does 116 and 117, it returned Richmond, Virginia and an unknown city in Missouri. Obviously, both locations are inaccurate as the subscriber is located in Blacksburg, Virginia.
 - d. I used several other geolocation websites and the location for the IP addresses for John Doe 116 and 117 always returned a location of Blacksburg, Virginia.
6. Plaintiff acknowledges that it does not know the identity of this John Doe. Armed only with the IP address of this John Doe’s device attached to the cable modem, it was impossible for Plaintiff to be able to ascertain the actual identity of this John Doe or that this John Doe “willfully and intentionally downloaded, copied, and distributed” the film in question or any other film.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on January 29, 2012.



John W. Simek