UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

THIRD DEGREE FILMS, INC. 20525 Nordhoff Street, Suite 25 Chatsworth, CA 91311 Plaintiff, v. DOES 1 – 216 Defendants.	)	Civil Action 1:11-cv-09618-PAE

I, Jon Nicolini, declare as follows:

1. I am the Vice President of Technology for Copyright Enforcement Group, LLC ("CEG").

2. CEG's address is 8484 Wilshire Boulevard, Suite 220, Beverly Hills, California 90211.

3. CEG is in the business of discovering infringements, and arranging for the enforcement, of the copyrights of its clients. Plaintiff in this case is a client of CEG. Based on information provided to me, I state that Plaintiff creates and distributes motion pictures, and the motion picture named Plaintiff's Complaint is among the motion pictures whose copyrights are the subject of the CEG's efforts on behalf of Plaintiff.

4. Music and motion picture piracy (i.e., the unauthorized copying and/or distribution of songs and motion pictures) has been a serious problem since at least as early as home audio and video tape cassette players became popular. The problem continued with the introduction of home CD and DVD players. Today the problem persists with the ability to store digital files of songs and motion pictures in the memory of home and/or laptop computers, and for people to distribute such files to each other over the Internet on peer-to-peer networks (sometimes called "P2P" networks) using file sharing software applications such as BitTorrent.

Articles describing aspects of music and motion picture piracy could be found, at least until recently, at these web pages, among others, on the Internet:

(1) http://www.usvo.com/usvo_videopiracy.pdf (attached to this Declaration as **Exhibit 1**), and

(2) http://www.thefreelibrary.com/DVD+piracy+in+the+U.S.+becomes+an+industry-a0103403775 (attached to this Declaration as **Exhibit 2**).

5. Neither of the two major operating systems for personal computers (i.e., those developed by Microsoft Corporation and Apple, Inc.) nor any of the four most used web browsers, namely, Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari, which are used by well over 90% of users in the United States, include native functionality for peer-to-peer file sharing over the Internet. (Regarding the relative popularity of browsers, see the following articles that could be found, at least until recently, at these web pages, among others, on the Internet,

http://gs.statcounter.com/#browser-US-monthly-201006-201106-bar (attached to this Declaration as **Exhibit 4**)

http://www.statowl.com/web_browser_market_share.php?1=1&timeframe=last_3&interval=month&chart_id=4&fltr_br=&fltr_os=&fltr_se=&fltr_cn=&timeframe=last_12 (attached to this Declaration as **Exhibit 5**).

Other than Microsoft Internet Explorer and Apple Safari, all other browsers must be intentionally installed. Therefore, the original seeder and each of the members of the swarm (i.e., each peer) must have separately installed on their respective computers special software that allows peer-to-peer sharing of files by way of the Internet. The most popular type of peer-to-peer file sharing program utilizes the BitTorrent protocol. The seeder and members of the swarm use software known in the field as "BitTorrent clients." Among the most popular BitTorrent clients are Vuze (formerly Azureus), µTorrent, Transmission and BitTorrent 7, although many others are used as well. In any event, the seeder and each member of the swarm (i.e., peer) must intentionally install a BitTorrent client (i.e., software application) onto his or her computer before that computer can be used to join a BitTorrent file sharing network.

6. P2P networks distribute infringing copies of motion pictures (and works in other forms such as music and books) with file sharing software such as BitTorrent as follows: The process begins with one user accessing the Internet through an Internet Service Provider ("ISP") and intentionally making a digital file of the work available on the Internet to the public from his or her computer. This first file is often referred to as the first "seed." I will refer to the person making this seed available as the "original seeder." Persons seeking to download such a work also access the Internet through an ISP (which may or may not be the same ISP as used by the original seeder) and seek out the work on a P2P network. With the availability of the seed, other users, who are referred to as "peers," access the Internet and request the file (by searching for its title or even searching for the torrent's "hash" - described below) and engage the original seeder and/or each other in a group, sometimes referred to as a "swarm," and begin downloading the seed file. In turn, as each peer receives portions of the seed, most often that peer makes those portions available to other peers in the swarm. Therefore, each peer in the swarm is at least copying and is usually distributing, as a follow-on seeder, copyrighted material at the same time. This also means that the participants engage in a series of related transactions. Of the over 20,000 infringers tracked in connection with several cases currently pending, at least 95% of the Doe defendants were uploading (i.e., distributing) illegal copies of our clients' motion pictures at the moment indicated by the Timestamp in the respective Exhibit A appended to each complaint, which is also true for this case. In P2P networks, the infringement may continue even after the original seeder has gone completely offline. Any BitTorrent client may be used to join a swarm. As more peers join a swarm at any one instant, they obtain the content at even greater speeds because of the increasing number of peers simultaneously offering the content as seeders themselves for unlawful distribution. As time goes on, the size of the swarm varies, yet it may endure for a long period, with some swarms enduring for 6 months to well over a year depending on the popularity of a particular motion picture. As a result, the original seed file becomes unlawfully duplicated multiple times by multiple parties, with a potentially exponential increase in the number of illegal copies of any copyrighted work. With respect to any particular swarm,

the hash (an alphanumeric representation of a digital file) associated with the copied file's torrent file remains the same.

7. The premise of BitTorrent sharing is well known, and is stated on the Bittorrent.com website, at least until recently here, http://www.bittorrent.com/help/guides/beginners-guide (attached to this Declaration as **Exhibit 6**) as follows:

> "BitTorrent is a protocol (a set of rules and description of how to do things) allowing you to download files quickly by allowing people downloading the file to upload (distribute) parts of it at the same time. BitTorrent is often used for distribution of very large files, very popular files and files available for free, as it is a lot cheaper, faster and more efficient to distribute files using BitTorrent than a regular download."

That is, each peer (i.e. member of a swarm) in a P2P network has acted and acts in cooperation with the other peers by agreeing to provide, and actually providing, an infringing reproduction of at least a substantial portion of a copyrighted work in anticipation of the other peers doing likewise with respect to that work and/or other works. Joining a P2P network is an intentional act, requiring the selection by a peer of multiple links to do so.

8. Depending on the particular P2P network involved, at any one time any number of people, from one or two, to hundreds, to several thousands, unlawfully use the P2P network to upload, that is, distribute, or download, that is, copy, copyrighted material. To the extent that persons using a P2P network identifies themselves, they use "user names" or "network names" which typically are nicknames that do not disclose the true identity of the user, and do not indicate the residence or business address of the user. So, while, as I explain below, we can detect infringements, we can only identify the infringers by their Internet Protocol address and the time that the infringement is detected by us. Note that while we detect an infringement at a particular instant, the infringer may, and likely is infringing at other times as well.

9. The use of P2P networks, such as those accessed with BitTorrent software, to make unauthorized copies of motion pictures has become such common knowledge that it is casually mentioned in newspaper articles. For example, in the article titled "The Glut of Shows

Unwatched" published on the New York Times website, and which at least until recently could be seen at this web page: http://www.nytimes.com/2010/09/06/business/media/06carr.html (attached to this Declaration as **Exhibit 3**). There is this statement by the article's author who was describing his efforts to find a television show he had missed:

> "Starting to feel desperate, I thought for a moment about hopping on the laptop and searching BitTorrent for an **illegal copy**, but given that I make a living creating original content for a large media company, **stealing** from another one did not seem like a good idea."

(Emphasis added by me.)

10. Plaintiff and other similarly situated companies contract with CEG to have CEG determine whether or not copies of their works are being distributed on the Internet without their permission and to identify infringers. Plaintiff does not authorize distribution of its motion pictures on P2P networks.

11. CEG utilizes a system of software components ("the System") conceptualized, developed, and maintained by me in order to collect data about unauthorized distribution of copies of copyrighted works on P2P networks.

12. The life cycle as it relates to monitoring copyrighted works of CEG's client's begins as follows. When a copyrighted work is requested to be monitored, my colleagues and I first check to ensure that a copyright registration exists for the work or is in process with the U.S. Copyright Office.

13. In this case, we confirmed that the work at issue in the above-captioned case (the "Work") is titled "Illegal Ass 2" and is registered in the United States Copyright Office (PA0001366719/2007-03-02), and that the Copyright Office's or other records show that the copyright is owned by the above-identified Plaintiff.

14. Once the copyright information is confirmed, we use a text-based search to find digital files on the Internet that have the same title as the copyrighted work.

15. The digital files for which we search are available on P2P networks. As described above, a person making a copy available on a P2P network typically had obtained his or her copy

from a P2P network, and whenever a digital file is located on anyone's computer on a P2P network, that digital file is typically available to be downloaded from that computer to a requestor's computer. In every case that a CEG client's motion picture is available on a P2P network, it is an unauthorized distribution of the motion picture.

16. In this case, the P2P network on which we found unauthorized distribution of Plaintiff's Work was a BitTorrent network.

17. When a digital file with the same name as CEG's client's motion picture is found on a P2P network, CEG downloads a full copy of the file. The file is then forwarded to a two-stage verification computer process and identified by two people. The computer process compares the digital data in the suspect file with digital data in a digital copy of the motion picture obtained from CEG's client. If the suspect file matches the authorized file, then the two people play the suspect file and watch the motion picture. If both people confirm that a substantial portion of the motion picture in the suspect file is substantially the same as a corresponding portion of CEG's client's motion picture, then particular unique data (often referred to as metadata) in the suspect file (now referred to in this Declaration as the "accused file") is noted by the System, and the System searches for additional computers on P2P networks that have the same suspect file.

18. Users subscribe to the services of an ISP to gain access to the Internet. Each time a subscriber accesses the Internet, the ISP provides a unique Internet Protocol ("IP") address to the subscriber. An ISP generally records the times and dates that it assigns each IP address to a subscriber and maintains for a period of time a record of such an assignment to a subscriber in logs maintained by the ISP. In addition, the ISP maintains records which typically include the name, one or more address, one or more telephone numbers, and one or more email addresses of the subscriber. P2P technology relies on the ability to identify the computers to and from which users can search and exchange files. The technology identifies those computers by the IP address from which the computer connects to the Internet. Taking advantage of this technology and the unique metadata associated with the file containing unlawful copy of CEG's client's

motion picture, CEG's System inspects file-sharing networks for computers that are distributing at least a substantial portion of a copy of a copyrighted work owned by Plaintiff, and when CEG finds such a computer, CEG's System also collects the following publicly accessible information: (a) the time and date the infringer was found, (b) the time(s) and date(s) when a portion of the accused file was downloaded successfully to the accused infringer's computer, (c) the time and date the infringer was last successfully connected to via the P2P network with respect to the infringer's computer's downloading and/or uploading the accused file to the Internet (hereinafter referred to as "Timestamp"), (d) the IP address assigned to the infringer's computer, (e) the P2P software application used by the infringer and the port number used by the infringer's P2P software, (f) the size of the accused file, and that file's MD5 checksum, and SHA-1 checksum (the last of which is the unique "hash" referred to above), (g) the percent of the file downloaded by us from the infringer's computer, (h) the percent of the accused file on the infringer's computer which is available at that moment for copying by other peers, and (i) any relevant transfer errors. In addition, CEG uses available databases to record the name of the ISP having control of the IP address and the state (and often the city or county) associated with that IP address. However, because of the partially anonymous nature of the P2P Internet distribution system used by Defendants, the true names, street addresses, telephone numbers and email addresses of Defendants are unknown to Plaintiff at this time. CEG also downloads the available file from a subscriber's computer, and later runs visual observations to confirm whether or not the file is a copy of at least a substantial portion of a copyrighted work of Plaintiff. CEG has confirmed that each of the files obtained from the Defendants that are listed in **Exhibit A** attached to the Complaint filed in this case is a copy of a substantial portion of the copyrighted work listed in **Exhibit A**. All of this information is stored in database files on CEG's computers.

19. As indicated above, an Internet Protocol address uniquely identifies each computer connected to the Internet. If one knows a computer's Internet Protocol address, one can, using publicly available reverse-lookup databases on the Internet, identify the ISP used by that computer and the city (or county) and state in which the computer was located at the date

and time that the Internet Protocol address was obtained. However, the actual name and address of the person subscribing to the ISP's service is neither publicly available, nor available to CEG.

20. However, with the Internet Protocol address and the date and time that the infringer's computer was accessing the Internet through the ISP, the ISP (be it AT&T, Verizon, Qwest, Comcast or any of many other ISPs) can review its own subscriber logs to identify either (i) the names and addresses of the subscriber, or (ii) the intermediary ISP through which the person is ultimately subscribed to the main ISP. In turn, if the intermediary ISP is provided with the Internet Protocol address and the date and time that the infringer's computer was accessing the Internet through the ISP, then the intermediary ISP can review its own subscriber logs to identify the name, addresses, telephone numbers and email addresses of the subscriber.

21. With respect to accused files, CEG sends notices (sometimes referred to as "DMCA notices") to ISPs. Each notice includes the identity of an accused file and the Internet Protocol address of the computer having that file available for download, along with the Timestamp associated with it. In the notice, CEG requests that the ISP forward the notice to the ISP's subscriber associated with the Internet Protocol address. Each notice includes, among other information, an address for the accused infringer to contact CEG to arrange for settlement. In the above-captioned case, the Internet Protocol addresses identified in **Exhibit A** of the Complaint are those of subscribers who had not settled with CEG. **Exhibit A** lists on a Defendant-by-Defendant basis (one Defendant per row) the IP address associated with each Defendant, the identity of the ISP associated with the IP address, the date and time (the Timestamp referred to earlier) that the infringement by that Defendant was last observed, and the software protocol used by the Defendant in infringing the Work, the title of which, along with its copyright registration number, is set forth on the first page of **Exhibit A.**

22. With respect to Plaintiff's copyrighted motion picture named in the Complaint, CEG performed the steps described in paragraphs 11-21 above. In summary, each of the computers having the IP addresses and time stamps listed in **Exhibit A** of the Complaint made a digital file copy of at least a substantial portion of Plaintiff's Work, and, without authorization,

made such file available for download by others on a P2P network. As indicated above, all of the infringers identified as "Doe" defendants in the Complaint used BitTorrent software. Further, the hashes associated with the torrent files on the computers having the IP addresses and time stamps listed in **Exhibit A** are all identical to each other, that is, they all have the same hash. This demonstrates that all the Doe defendants listed in **Exhibit A** joined the same swarm and engaged in a series of related transactions.

23. CEG sent DMCA notices as described above to the ISPs with respect to all the Doe Defendants in the case. None of the ISPs provided the names and addresses of the Doe Defendants to CEG. However, we could determine that the Doe Defendants in this case are likely within or near the geographic location of the court. Without information held by the ISPs, we cannot obtain further information needed to identify the Defendants, including their names, and their actual addresses, telephone numbers and email addresses.

24. In sum, the Defendants in this case engaged in a series of related transactions, because they all downloaded the exact same file (not just the same copyrighted work), within a limited period of time. Furthermore, because of the nature of torrent software, they engaged in a series of related transactions because in order to download a movie (or parts of it), one must permit other users to download and/or upload the file from one's own computer. Thus, the Defendants were simultaneously trading (downloading and/or uploading) the exact same file during a limited period of time. While Defendants engaged in this downloading and/or uploading of the file, they exposed their IP address. With torrent software, one can see the IP address of the various computers that one is connected to, and which are sharing files in cooperation with, one's own computer.

25. We have made every effort to ensure that all alleged infringers have in fact engaged in a series of related transactions and can thus be properly joined in one lawsuit. Most importantly: (i) We have identified only alleged infringers who traded exactly the same file of the copyrighted works at issue (not just the same copyrighted work); and (ii) we have limited the time period during which we searched copyright infringements; in addition, (iii) we have limited

the geographic search to ensure as much as technically possible that the alleged infringers are in fact within the geographic area of the court. However, because of intermediary ISPs and the location of the ISPs technical facilities, the location cannot always be exactly pinpointed.

26. I am informed that before any discovery can be made in civil litigation, a meeting of the parties or the parties' counsel must be held. However, the actual identities of the Doe Defendants are unknown to Plaintiff, and therefore cannot be served. Without serving the Complaint on any defendant, the pre-discovery meeting cannot be held. Therefore, Plaintiff needs early discovery from the ISPs, and any intermediary ISPs that may be involved, so that the names and addresses of the accused infringers can be obtained by Plaintiff to enable it to enforce its rights in its copyright and prevent continued infringement.

27. ISPs retain their logs for only a limited time. In my experience, based on my three years of hands-on experience in working with ISPs, such information is retained for only about six months. Thus, such information must be requested expeditiously and the ISP must be informed to retain such information in view of subsequent litigation.

28. I declare under penalty of perjury that the foregoing is true and correct of my own personal knowledge, except for those matters stated as information and belief, and those matters I believe to be true, and if called upon to testify I can competently do so as set forth above.

Executed this 23rd day of December, 2011 in Los Angeles, California.

Jon Nicolini

EXHIBIT 1

TO DECLARATION OF JON NICOLINI

EXHIBIT 2

TO DECLARATION OF JON NICOLINI

EXHIBIT 3

TO DECLARATION OF JON NICOLINI

EXHIBIT 4

TO DECLARATION OF JON NICOLINI

EXHIBIT 5

TO DECLARATION OF JON NICOLINI

EXHIBIT 6

TO DECLARATION OF JON NICOLINI