IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHER DISTRICT OF ILLINOIS, EASTERN DIVISION

Zambezia Film (Pty) Ltd., A South African Corporation *Plaintiff,*	)	
v.	)	Case No.
DOES 1-65 *Defendants.*	)	***JURY TRIAL DEMANDED***

DECLARATION OF DARREN M GRIFFIN IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

1. My name is Darren M Griffin. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

2. I have been retained as a software consultant by Crystal Bay Corporation CBC ("CBC"), a company incorporated in South Dakota and organized and existing under the laws of the United States, in its technical department. CBC is in the business of providing forensic investigation services to copyright owners.

3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data.

4. Unfortunately, the Internet also has afforded opportunities for the wide-scale infringement of copyrighted motion pictures.

5. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called P2P networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material.

8. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed.

9. Further, a person who uses a P2P network is free to use any alias (or "network name") whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies for which Crystal Bay Corporation monitored for Plaintiff's Motion Picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally

elects to share a file using a P2P network. This is called "seeding." Other users ("peers") on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or "swarm") from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole.

11. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a P2P network—or even a portion of a copy—can also be a source of download for that infringing file, potentially both copying and distributing the infringing work. This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence is then saved on Crystal Bay Corporation's service.

14. Once Crystal Bay Corporation's searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, Crystal Bay Corporation obtains the IP address of a user offering the file for download.

15. The forensic software used by CBC routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works.

16. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). It only enables Crystal Bay Corporation to trace the infringer's access to the Internet to a particular ISP. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

17. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the user/subscriber.

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber.

19. When available, Crystal Bay Corporation also obtains the user's pseudonym or network name and examines the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's Motion Picture. In addition to the file of the motion picture itself, Crystal Bay Corporation downloads or otherwise collects publicly available information about the network user that is designed to help Plaintiff identify the infringer.

20. The exact manner in which Crystal Bay Corporation determines a user's IP address varies by P2P network.

21. Crystal Bay Corporation determined that the Doe Defendants here were using ISPs listed in Exhibit B to Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference, together with various other ISPs operating both within and outside the Northern District of Illinois, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

22. Once Crystal Bay Corporation identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, an e-mail was sent to the relevant contact at each ISP informing them of the Doe Defendant's IP address and the date and time of the infringing activity.

23. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay Corporation (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves.

24. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Crystal Bay Corporation watches a DVD copy of the Motion Picture provided by Plaintiff.

25. After Crystal Bay Corporation identified the Doe Defendants and downloaded the motion pictures they were distributing, Crystal Bay Corporation opened the downloaded files, watched them and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

26. Plaintiff retained CBC to identify the IP addresses of those BitTorrent users who

were copying and distributing Plaintiff's copyrighted audiovisual work as identified in Exhibit B (the "Work"). CBC tasked me with analyzing, reviewing and attesting to the results of the investigation.

27. During the performance of my duties as detailed below, I used forensic software provided by CBC to scan peer-to-peer networks for the presence of infringing transactions.

28. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Work.

29. Through each of the transactions, the computers using the IP addresses identified in Exhibit B transmitted a copy or a part of a copy of a digital media file identified by the hash value set forth in Exhibit B. The IP addresses, hash values, dates and times contained in Exhibit B correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Exhibit B were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the copyrighted work identified in Exhibit B.

30. Moreover, the users were sharing the exact same copy of the Work. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a US government standard. Using a hash tag to identify different copies of the Work, I confirmed that these users reproduced the very same copy of the Work.

31. The CBC software analyzed each BitTorrent "piece" distributed by each IP address listed in Exhibit B and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

32. The software uses a geolocation functionality to confirm that all IP addresses of

the users set forth in Exhibit B were located in Ohio. Though an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

33. As set forth in Exhibit A, I have confirmed not only that the users distributed the files in Ohio, but also the specific location where the distribution took place.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 21st day of February, 2013.

By: _____
Darren M Griffin

60998770.1