UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

BREAKING GLASS PICTURES, LLC,

Plaintiff,

CASE NO.: 8:13-CV-01154-JDW-TBM

v.

DOE 49,

Defendant.
_____/

DECLARATION OF DARREN M. GRIFFIN IN SUPPORT OF BREAKING GLASS PICTURES, LLC'S MOTION FOR LEAVE TO SERVE NON-PARTY SUBPOENA PRIOR TO RULE 26(f) CONFERENCE AND SUPPORTING MEMORANDUM OF LAW

I, Darren M. Griffin, declare:

1. I work for Crystal Bay Cooperation CBC, "Crystal Bay", a company incorporated in South Dakota with its principal address at 110E Center Street, Suite 2013, Madison, South Dakota 57042. Crystal Bay is a provider of online anti-piracy services for the motion picture industry. Before my employment with Crystal Bay, I held various positions at companies that developed software technologies. I have approximately ten years of experience related to digital media and computer technology.

2. I submit this declaration in support of Plaintiff's Motion for Leave to Serve Non-Party Subpoenas Prior to Rule 26(f) Conference. This declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

EXHIBIT B
6 Degrees 3-49

3. At Crystal Bay, I am the head of the department that carries out evidence collection and provides litigation support services. I work closely with our research team to create credible processes to scan for, detect, and download copies of copyrighted material on multiple network protocols for use by copyright owners.

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

5. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called "peer-to-peer" ("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 or peers; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

6. On behalf of Plaintiff, we engaged in a specific process using Crystal Bay's specially designed software technology to identify direct infringers of Plaintiff's

copyrighted materials using protocols investigated by Crystal Bay's software on P2P networks. Crystal Bay has documented evidence of the unauthorized reproduction and distribution of the copyrighted motion picture to which Plaintiff holds the exclusive distribution and licensing rights, *6 Degrees of Hell* (the "Motion Picture"), within the United States of America, including the Middle District of Florida.

7. Because the Plaintiff has not authorized its copyrighted Motion Picture to be copied or distributed in unsecured P2P networks, I believe that the copying and distribution of the Motion Picture on P2P networks violates the copyright laws.

8. Crystal Bay has licensed a proprietary technology that provides an effective means to detect the unauthorized distribution of movies and other content and files over online media distribution systems, or P2P networks. Crystal Bay's technology enables it to detect and monitor the unlawful transfer and distribution of files amongst the P2P networks by different protocols. Those protocols 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 with P2P networks. This is called "seeding." Other users ("peers") on the network connect to the seed file to download.

9. The particular P2P protocol at issue in this suit is called "BitTorrent." What makes BitTorrent unique is that, as yet additional peers request the same file, each additional user becomes a part of the network from where the file can be downloaded. However, unlike a traditional P2P network, each new file downloader is receiving a portion of the data from each connected user who has already downloaded a part of the file that together comprises the whole. This means that every "node" or user who has a

copy of the infringing copyrighted material on a P2P network investigated by our software must necessarily also be a source of download for that infringing file.

10. Specifically, the BitTorrent process works as follows: Users intentionally download a small program that they install on their computers – the BitTorrent "client" application. The BitTorrent client is the user's interface during the downloading/uploading process. There are many different BitTorrent clients, all of which are readily available on the Internet for free.

11. BitTorrent client applications typically lack the ability to search for torrent files. To find torrent files available for download (as made available by other BitTorrent users), users intentionally visit torrent sites using any standard web browser

12. A torrent site is a website that contains an index of torrent files being made available by other users (generally an extensive listing of movies and television programs, among other copyrighted content). The torrent site hosts and distributes these small torrent files. Although torrent files do not contain actual audio/visual media, they instruct a user's computer where to go and how to get the desired file. In essence, the torrent file contains a "roadmap" to the IP addresses of other users who are sharing the media file identified by the unique has identifier, as well as specifics about the media file. Torrent files interact with specific trackers, allowing the user to download the desired file.

13. The torrent file contains a unique hash identifier, which is a unique identifier generated by a mathematical algorithm developed by the National Security Agency. This torrent file is tagged with the file's unique "info-hash," which acts as a

"roadmap" to the addresses of other users who are sharing the media file identified by the unique info-hash, as well as specifics about the media file. The hash identifier of the torrent files utilized by Doe 49 and its peers to illegally distribute and share Plaintiff's Motion Picture is as follows:

SHA1: 9121709D661CCE40115180C4B6CCC4E496B8CF8E ("Hash SHA1: 9121").

14. A BitTorrent tracker manages the distribution of files, connecting uploaders (those who are distributing content) with downloaders (those who are copying the content). A tracker directs a BitTorrent user's computer to other users who have a particular file, and then facilitates the download process from those users. When a BitTorrent user seeks to download a movie or television file, he or she merely clicks on the appropriate hash file on a torrent site, and the torrent file instructs the client software how to connect to a tracker that will identify where the file is available to begin downloading it. In addition to a tracker, a user can manage file distribution through a Distributed Hash Table. Furthermore, a so-called Peer-Exchange is used to retrieve more users for the specific file.

15. Files downloaded in this method are downloaded in hundreds of individual pieces. Each piece that is downloaded is immediately thereafter made available for distribution to other users seeking the same file. The effect of this technology makes every downloader also an uploader of the content. This means that every user who has a copy of the infringing material on a torrent network must necessarily also be a source of download for that material.

16. In order to have engaged in the unauthorized distribution and sharing of Plaintiff's copyrighted Motion Picture, each of the participating peers intentionally obtained a torrent file for Plaintiff's Motion Picture from the video index of a BitTorrent website or other torrent site. Each of the participating peers then intentionally loaded that torrent file into a computer program downloaded onto their computer that is specifically designed to read such files. With the torrent file loaded, the BitTorrent program employed the BitTorrent protocol to initiate simultaneous connections to hundreds of other peers possessing and sharing copies of the digital media – Plaintiff's Motion Picture – described in the torrent file.

17. Once connected, the program began coordinating the copying of Plaintiff's Motion Picture among participating peer computers. As the film was copied to the peers' computers piece by piece, the downloaded pieces were immediately made available to other connected peers seeking to obtain the file.

18. Each of the peers is a member of a single "swarm" or group of BitTorrent peers whose computers are collectively connected for the sharing of a particular hash file, in this instance, Plaintiff's Motion Picture, and this swarm is associated with is the foregoing unique hash identifier.

19. Peer Exchange is a communications protocol built into almost every BitTorrent protocol which allows swarm members to share files more quickly and efficiently. Peer Exchange is responsible for helping all other swarm members participate in illegal file sharing, regardless of geographical boundaries.

20. A Distributed Hash Table is a sort of world-wide telephone book, which uses each file's "info-hash" (a unique identifier for each torrent file) to locate sources for the requested data. Thus, swarm members are able to access a partial list of swarm members rather than being filtered through a central computer called a tracker. By allowing members of the swarm to rely on individual computers for information, this not only reduces the load on the central tracker, but also means that every client that is sharing this data is also helping to hold this worldwide network together.

21. Each of the peers participated in the swarm for the purpose of the reproduction and distribution of Plaintiff's Motion Picture.

22. The distributed nature of the P2P networks typically leads to a rapid viral spreading of a file throughout peer users. As more peers join the collective swarm, the frequency of successful downloads also increases. Because of the nature of a BitTorrent protocol, any user who has downloaded a file prior to the time that subsequent user downloads the same file is automatically a source for the subsequent peer, so long as that first user is online at the time the subsequent user request the file from the swarm. Because of the nature of the swarm, every infringer is – and by necessity all infringers together are – simultaneously both stealing the Plaintiff's copyrighted material and redistributing it. Millions of people have used P2P networks to distribute copyrighted material.

23. Crystal Bay used the search function of the P2P network to look for network users who were offering for distribution audiovisual files that were labeled with the names of Plaintiff's copyrighted Motion Picture. Crystal Bay then conducted a

download of the respective content and a careful and thorough review of that data. The unique hash identifier of the file was extracted from the original torrent file as soon as the content had been verified as a valid copy of Plaintiff's copyrighted Motion Picture. Crystal Bay started searching for individuals making the content identified by the hash value available to the public. When a network user was located who was making that content available for distribution, Crystal Bay downloaded a part of the that file and stored other specific information in order to confirm that infringement was occurring and to identify the infringer by the unique Internet Protocol ("IP") address assigned to Doe 49 by his/her ISP on the date and at the time of the Doe 49's infringing activity.

24. Doe 49 and its peer infringers in the swarm were identified in the following way: Crystal Bay's software is connected to the *6 Degrees of Hell* file, an illegal version of the Motion Picture. All infringers connected to the file will be investigated through downloading a part of the file placed on their computer. This evidence is saved on our server and could be shown to the court as evidence if necessary.

25. Once Crystal Bay'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, we obtain the Internet Protocol ("IP") address of a user offering the file for download. In addition to the file of the motion picture itself, we download or otherwise collect publicly available information about the network user that is designed to help Plaintiff identify the infringer. Among other things, we download or record for each file downloaded: (a) the time and date at which the file or a part of the file was distributed by the user; (b) the IP address assigned to each user at the time of

infringement; (c) the ISP for each infringer; (d) the BitTorrent client application used by each user; (e) the global unique identifier for each file downloaded by each user; (f) the location of most users (by state) at the time of download as determined by geolocation technology; and, in some cases, (g) the video file's metadata (digital data about the file), such as title and file size, that is not part of the actual video content, but that is attached to the digital file and helps identify the content of the file. We then create evidence logs for each user and store all this information in a database.

The Need for Expedited Discovery

26. Obtaining the identity of copyright infringers, including Doe 49, on an expedited basis is critical to prosecution of this action and stopping the continued infringement of this copyrighted motion picture. Without expedited discovery in the instant case, Plaintiff has no way of serving Doe 49 with the complaint and summons in this case. Plaintiff does not have Doe 49's name, address, e-mail address, telephone number, or any other way to identify or locate Doe 49, other than the unique IP address assigned to Doe 49 by his/her Internet Service Provider on the date and at the time of Doe 49's infringing activity.

27. Further, Internet Service Providers ("ISPs") have different policies pertaining to the length of time they preserve session data which identifies their subscribers. Despite requests to preserve the information, some ISPs keep the session data of their subscribers' activities for only limited periods of time – sometimes as little as weeks or even days – before erasing the data they contain. If an ISP does not have to

respond expeditiously to a discovery request, the identification in that ISP's logs may be erased.

28. An IP address is, in combination with the date, a unique numerical identifier that is automatically assigned to a user by its ISP each time a user logs on to the network. Each time a subscriber logs on, he or she may be assigned a different IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses. ISPs keep track of the IP addresses assigned to its subscribers at any given moment and retain such "user logs" for a very limited amount of time. These user logs provide the most accurate means to connect an infringer's identity to its infringing activity.

29. Although users' IP addresses are not automatically displayed on the P2P networks, any user's IP address is readily identifiable from the packets of data being exchanged. The exact manner in which we determine a user's IP address varies by P2P network.

30. An infringer's IP address is significant because it becomes a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer using the Internet. However, the IP address does not enable us to ascertain with certainty the exact physical location of the computer or to determine the infringer's identity. It only enables us to trace the infringer's access to the Internet to a particular ISP and, in some instances, to a general geographic area. 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.

31. Here, the IP address Crystal Bay identified for Plaintiff enabled us to determine which ISP was used by Doe 49 to gain access to the Internet. Publicly available databases located on the Internet list the IP address ranges assigned to various ISPs. However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. Since these ISPs consequently have no direct relationship – customer, contractual, or otherwise – with the end-user, they are unable to identify the infringers through reference to their user logs. The intermediary ISP's own user logs, however, should permit identification of Doe 49. We determined that Doe 49 was using the ISP listed in Exhibit A to Plaintiff's Motion, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted Motion Picture.

32. We downloaded the entire copyrighted Motion Picture, and other identifying information described above, reviewed it and added such information to our monitoring system. Subsequently, we created evidence logs for a small part of the motion picture file for Doe 49. Once the ISP is provided with the IP address, plus the date and time of the infringing activity, Doe 49's ISP quickly and easily can use its subscriber logs to identify the name and address of the ISP subscriber who was assigned that IP address at that date and time.

Confirmation of Downloaded Material

33. I am also responsible for identifying on-line piracy of motion pictures for Crystal Bay, including gathering evidence of on-line piracy to support counsel's copyrighted protection enforcement efforts.

34. As part of my responsibilities at Crystal Bay, I have been designated to confirm that the digital audiovisual files downloaded by Crystal Bay are actual copies of Plaintiff's Motion Picture. It is possible for digital files to be mislabeled or corrupted; therefore, Crystal Bay (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 itself.

35. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, one of my assistants or I have watched a copy of the Motion Picture provided by Plaintiff. The downloaded files have been carefully reviewed and compared by a visual comparison with the original motion picture. We have confirmed that they contain a substantial portion of the Motion Picture identified in the Complaint and that at least the Motion Picture DVD case displays a copyright notice.

36. Plaintiff's Motion Picture continues to be made available for unlawful transfer and distribution using P2P protocols, in violation of Plaintiff's exclusive licensing and distribution rights, and rights in the copyright. Crystal Bay continues to monitor such unlawful distribution and transfer of Plaintiff's Motion Picture and to identify infringers.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on August 20, 2013

Darren M. Griffin