

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

ACHTE/NEUNTE BOLL KINO )
BETEILIGUNGS GMBH & CO KG )
Plaintiff, )
v. ) CA. 1:10-cv-00453-RMC
DOES 1 – 2,094 )
Defendants. ) Next Deadline: N/A

DECLARATION OF PATRICK ACHACHE IN SUPPORT OF PLAINTIFF’S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

I, Patrick Achache, declare:

1. I am Director of Data Services for Guardaley, Limited (“Guardaley”), a company incorporated in England and Wales under company number 06576149, where I have been employed since January of 2007. Guardaley is a leading provider of online anti-piracy services for the motion picture industry. Before my employment with Guardaley, I held various software developer and consultant positions at companies that developed software technologies. I have approximately ten (10) years of experience related to the protocols, technical architecture and operation of the Internet.

2. I submit this declaration in support of Plaintiff’s Motion for Leave to Take Discovery 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.

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

4. Guardaley has developed a proprietary technology platform that provides an effective means to detect the unauthorized distribution of movies and other audiovisual content and files over online media distribution systems, or “peer-to-peer” (“P2P”) networks. Guardaley’s technology enables it to detect and monitor the unlawful transfer and distribution of files amongst the P2P network by a “BitTorrent protocol” or “torrent” which is different than the standard P2P protocol used for such networks as Kazaa and Limewire. The BitTorrent protocol makes 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 a torrent network. This initial file is called a “seed”. Other users (“peers”) on the network connect to the seed file to download. 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 different piece of the data from each user who has already downloaded the file that together comprise the whole (this piecemeal system with multiple pieces of data coming from peer members is called a “swarm”). So every downloader is also an uploader. This means that every “node” or peer user who has a copy of the infringing copyrighted material on a torrent network must necessarily also be a source of download for that infringing file.

5. This distributed nature of BitTorrent 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 BitTorrent protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file. Essentially, because of the nature of the swarm downloads as described above, every infringer is

*simultaneously* stealing copyrighted material from many ISPs in numerous jurisdictions around the country.

6. The Plaintiff in this action is producer and distributor of motion pictures. The Plaintiff engaged the United States Copyright Group to, among other tasks, document evidence of the unauthorized reproduction and distribution of the copyrighted motion picture to which Plaintiff holds the exclusive distribution and licensing rights, "*Far Cry*", within the United States of America, including the District of Columbia.

7. USCG, in turn, retained Guardaley to monitor and identify copyright infringement of Plaintiff's copyrighted motion picture on P2P networks. On behalf of Plaintiff, we engaged in a specific process utilizing Guardaley's specially designed software technology to identify direct infringers of Plaintiff's copyright using BitTorrent protocol on P2P networks.

8. All of the torrent infringers named as Doe Defendants were identified in one of two ways. We either: (1) searched for files corresponding to Plaintiff's motion picture title "*Far Cry*" and then identified the users who are offering the files for unlawful transfer or distribution; or (2) reviewed server logs obtained from P2P networks to determine the users who were offering the files of this copyrighted movie. In the first identification method, we used the same core technical processes that are used by the P2P users on each respective network to identify users who are offering the "*Far Cry*" motion picture files on the network, or to directly locate the files of the film. In the second identification method, we reviewed the same data that would be available to the operator of a server that is part of the P2P network. Under the first method of identification, any user of a P2P network can obtain the information that is obtained by us from the P2P network. Under the second method of identification, any operator of a server that is part of the P2P network can obtain the information that is obtained by us from the P2P network.

9. Once Guardaley's searching software program identifies a file that is being offered for distribution using BitTorrent protocol that corresponds to the motion picture for which Plaintiff owns the exclusive licensing and distribution rights, "*Far Cry*", or once such a file is identified directly from our search or our review of server logs, we obtain the Internet Protocol ("IP") address of a user offering the file for download. When available, we also obtain the user's pseudonym or network name and examine the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's motion picture. We then download the motion picture that the user is offering using BitTorrent Protocol. In addition to the torrent 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 was distributed by the user; (b) the IP address assigned to each user at the time of infringement; and, in some cases, (c) 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 that store all this information in a central database.

10. An IP address is a unique numerical identifier that is automatically assigned to a user by its Internet Service Provider ("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.

11. 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.

12. An infringer's IP address is significant because it is 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.

13. Here, the IP addresses Guardaley identified for Plaintiff enable us to determine which ISP was used by each infringer 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 Doe Defendants through reference to their user logs. The intermediary ISPs' own user logs, however, should permit identification of the Doe Defendants. We determined that the Doe Defendants here were using those ISPs listed in Exhibit A to the Complaint filed in this matter together with various other ISPs operating both

within and outside the District of Columbia, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

14. We downloaded the motion picture file and other identifying information described above and created evidence logs for each Doe Defendant. Once we identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, USCG sent an e-mail 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. That e-mail message requested that each ISP retain the records necessary to identify its subscriber who was assigned that IP address at that date and time. Once provided with the IP address, plus the date and time of the infringing activity, the Doe Defendant's ISPs quickly and easily can use their respective 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**

15. I am also responsible for identifying on-line piracy of motion pictures for Guardaley, including gathering evidence of on-line piracy to support counsel's copyright protection enforcement efforts.

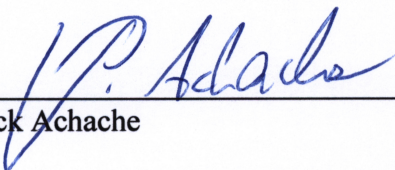
16. As part of my responsibilities at Guardaley, I have been designated to confirm that the digital audiovisual files downloaded by Guardaley are actual copies of the motion picture entitled "*Far Cry*". It is possible for digital files to be mislabeled or corrupted; therefore, Guardaley (and accordingly, 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.

17. As to Plaintiff's copyrighted motion picture entitled "*Far Cry*", as identified in the Complaint, I or one of my assistants have watched a DVD or VHS copy of the motion picture provided by Plaintiff. After Guardaley identified the Doe Defendants and downloaded the motion pictures they were distributing, we accessed the downloaded files using Guardaley's proprietary software application, which stores the files downloaded. We opened the downloaded files, watched them and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

18. Plaintiff's motion picture entitled "*Far Cry*" continues to be made available for unlawful transfer and distribution using BitTorrent protocol, in violation of Plaintiff's exclusive licensing and distribution rights, and rights in the copyright. USCG and Guardaley continue to monitor, on an on-going and continuing basis, such unlawful distribution and transfer of Plaintiff's motion picture and to identify infringers by the unique Internet Protocol ("IP") address assigned to them by their respective ISPs on the date and at the time of the infringing activity.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on 31.12.09, \_\_\_\_\_, at Karlsruhe.

  
\_\_\_\_\_  
Patrick Achache