DECLARATION OF MICHAEL PATZER

1. My name is Michael Patzer.

2. I am over the age of 18 and competent to make this declaration. The facts stated in this declaration are based upon my personal knowledge.

3. I went to Neumarkt i.d.Opf for high school in Germany and graduated from there in 1999.

4. I have worked in the Information Technology business since 1999.

5. I am currently an independent contractor for Excipio GmbH ("Excipio"), a German company located at Karlstrasse 49, 76133 Karlruhe, Germany, Phone Number: +49 (721) 354 801 – 00.

6. I designed, implemented, maintain, and monitor the data collection system that Excipio both owns and uses to identify the IP addresses used by people to commit copyright infringement via the BitTorrent protocol.

7. Excipio licenses this data collection system to IPP International UG ("IPP").

8. It took over a year to develop the proprietary software and system used by Excipio.

9. The data collection system used by IPP has the following components:

   a. a proprietary BitTorrent Client;

   b. a proprietary program analyzing the BitTorrent traffic and writes infringing transactions to a database;

   c. servers running a MySQL database cluster which log verified infringing transactions;

   d. packet analyzers, also known as packet sniffers, which create and analyze PCAPs;

MP

e. servers that run the proprietary BitTorrent Client, the BitTorrent analyzer and record PCAPs;

f. WORM ("Write Once Read Many") tape drives for storing the PCAPs, the torrent data and MySQL server data;

g. a program to synchronize the servers' clocks with both a GPS clock and an atom clock;

h. a proprietary program for checking the MySQL log files against the contents of the PCAPs; and

i. a proprietary program which checks the information contained in an Excel Spreadsheet against what is in the PCAPs and server's log files.

10. Excipio's data collection system accurately collected and recorded evidence proving that the defendant infringed Plaintiff's copyrighted work(s).

11. The first step in the evidence collection process is for the Plaintiff, here Malibu Media, LLC, to provide Excipio with the titles of the copyrighted content. This is done by IPP.

12. Excipio then conducts a lexical search for the titles on well-known torrent websites. Torrent websites host torrent files. To download content through BitTorrent a user will first download a BitTorrent client (software that enables the BitTorrent protocol work), and then search for torrent files on torrent websites. The BitTorrent client is then used to download the torrent file from the website.

13. When Excipio's lexical search yields matches, Excipio downloads the torrent files and joins the swarms of BitTorrent peers distributing a computer file – here, copies of Plaintiff's copyrighted movie(s). The peers in a BitTorrent swarm connect to each other's computers in order to transmit "pieces" of the computer file. Every "piece" of the computer file – and the

MP

entire computer file – transmitted via BitTorrent has its own unique hash value. A hash value is a digital fingerprint for a piece of data.

14. Excipio uses a proprietary BitTorrent client to connect to the swarm of infringers unlawfully sharing Plaintiff's copyrighted movies. Once Excipio has joined the swarm, its system begins logging the infringing transactions with BitTorrent peers. The software *does not* upload or distribute content; it was created such that it is incapable of doing so.

15. Excipio's system connects to the infringing peers using a TCP/IP connection. This connection cannot be spoofed. Once the connection is established, the system begins the process of downloading a piece or pieces of the infringing computer file from the computer connected to the internet through the Defendant's IP address. The entire process and all of the transactions are recorded and stored in Excipio's database.

16. Data sent through the internet is delivered in the form of "packets" of information. PCAP stands for "Packet Capture." A PCAP is a computer file containing captured or recorded data transmitted between two computers. A "Packet Analyzer" records packets of data being transmitted between two computers over a network, such as the internet, and saves it in a PCAP. Packet analyzers also enable users to read and analyze PCAPs. PCAPs are akin to videotapes, but instead of recording light and sound they record zeroes and ones.

17. Excipio's data collection system uses a proprietary packet analyzer and TCPDump (a free open-source packet analyzer) to record the infringing transactions in PCAPs. Both of these were in good working order at the time the PCAP was captured and recorded.

18. TCPDump is widely used and is capable of accurately recording network traffic flowing to and from a computer in the form of PCAPs.

19. Here, the PCAPs are recordings of numerous BitTorrent computer transactions

MP

during which a person using Defendant's IP Address sent pieces of an infringing computer file (which contain an unlawful copy of Plaintiff's works) to Excipio's servers. I personally maintain and monitor the servers.

20. Each PCAP clearly shows the IP address distributing the BitTorrent piece (Defendant's IP address), the IP address receiving the BitTorrent piece (Excipio's IP address), what was transmitted (a piece of Malibu Media's copyrighted movie(s)), the transaction protocol (*i.e.* BitTorrent), and the time of the infringing transaction.

21. Each infringing transaction is also recorded on a MySQL server log file. *See* Excel Containing MySQL data, attached hereto as Exhibit "A." Each entry on the MySQL log file correlates to a specific PCAP file in Excipio's possession.

22. The MySQL log file was created by a MySQL database which I installed and which was in good working order at the time the data was logged.

23. The PCAPs and MySQL server log files are saved onto WORM tape drives. WORM stands for "write once read many". Excipio uses these because it is impossible to modify or delete the data after it has been written to a WORM tape drive. Indeed, the WORM tape drive is not capable of being manipulated or altered. And, the only way to destroy the data is to destroy the WORM tape drive itself.

24. Each of the WORM tape drives is electronically stamped with a German government issued time stamp at least every twenty four hours.

25. The drives are then stored in a computer safe for safekeeping.

26. When the PCAP and MySQL log file evidence is provided to a party, the WORM tape drive on which the evidence was written and stored is located and the data then digitally restored. If asked, I could and would bring the actual computer files to trial in this matter.

MP

27. Only 1 PCAP per movie infringed is produced to the Plaintiff usually. 1 PCAP per movie is sufficient to prove without question that the infringement of each of the movies at issue occurred. Producing *all* PCAPs for each of the infringed movies would be superfluous and extremely time consuming.

28. In addition to producing 1 PCAP per movie and the MySQL server log file, I also produce the following:

a. One (1) Technical Report per movie. The Technical Reports are included merely for ease of reference and only translate the electronic data contained in the PCAPs to an easy to understand format. The first part of the Technical Report lists *all* of the infringing transactions committed by someone using Defendant's IP address for the specific movie. Each line correlates to a line of the MySQL log file. As previously stated, Excipio has a PCAP for each entry on the MySQL log file. The second part of the Technical Report pertains to the specific PCAP that was produced for that movie. The relevant lines from the PCAP are reproduced and explained in the Technical Report. Because PCAPs actually contain hundreds of different fields, reproducing only the relevant lines of the PCAP in the Technical Report makes the PCAP easier to understand. Highlighting the relevant lines in no way changes what the PCAP says but instead, merely points to the relevant information in the computer file which shows that someone using Defendant's IP address sent a piece of Plaintiff's copyrighted work to Excipio's servers.

b. One .tar file for each work infringed. The .tar files contain the actual media files Defendant's IP address was distributing (i.e. the unlawful copy of Plaintiff's movie).

MP

c. One .torrent file for each work infringed. The .torrent file is the computer file which allows the BitTorrent user's BitTorrent client to locate tracker computers within the peer-to-peer network and connect to the swarm.

29. A distributed hash table (DHT) is a class of a decentralized distributed system that provides a lookup service similar to a hash table: (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. Responsibility for maintaining the mapping from keys to values is distributed among the nodes, in such a way that a change in the set of participants causes a minimal amount of disruption. This allows a DHT to scale to extremely large numbers of nodes and to handle continual node arrivals, departures, and failures. BitTorrent clients use a "Distributed Hash Table" (DHT) to locate peers who are downloading a torrent file. Specifically, a BitTorrent client locates and connects to the DHT. After the DHT locates peers, it requests the IP address for each peer. Using this process BitTorrent users are able to locate and connect to a number of peers within a particular swarm.

30. Excipio's infringement detection system uses servers which are programmed to crawl popular torrent websites. In the process, the servers locate third party torrent files. The servers subsequently download the torrent files from these websites. Similar to BitTorrent clients, Excipio's system uses a DHT to obtain the IP Addresses of peers registered to each torrent file. Excipio's system uses nodes to locate peers downloading a specific torrent-file. After locating the peers, Excipio's system requests a list of all the registered peers within the swarm. All responses are saved in a database. This includes the IP addresses, dates, hash values, and file names corresponding to the torrent-files.

MP

31. The results of a search within the database for Defendant's IP address are attached hereto as Exhibit "B." The database records show Defendant's IP address was a registered peer within the swarms for each of the third party works listed on Exhibit B.

32. During the previous four (4) years, I have testified as a fact witness in the following cases:

a. *Malibu Media, LLC v. JOHN DOES 1, 6, 13, 14, and Bryan White*, 2:12-cv-02078-MMB (E.D. Pa. 2012) (Consolidated from Cases: 2:12-cv-02078-MMB, 2:12-cv-02078-MMB, 5:12-cv-02088-MMB)—Gave trial testimony essentially identical to the information contained in this declaration.

b. *Malibu Media, LLC v. Michael Harrison*, 1:12-cv-01117-WTL-MJD (S.D. Ind. 2014) – Gave testimony essentially identical to the information contained in this declaration.

c. *Malibu Media, LLC v. Kelley Tashiro and N. Charles Tashiro*, 1:13-cv-00205-WTL-MJD (S.D. Ind. 2015) – Gave testimony essentially identical to the information contained in this declaration.

33. I am not paid by Malibu Media, LLC for my testimony in this matter.

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 this 28th day of July, 2015.

By:_____

MICHAEL PATZER

MP