EXHIBIT 1

Percipient Witness Statement of Chris Connelly

Professional Experience and Background

I, Chris Connelly, Director of Data Collection, currently work for Peer Media Technologies, Inc. Peer Media Technologies (PMT) is the leading provider of content protection, copyright enforcement and digital piracy measurement services for companies in the entertainment, software and publishing industries. I have been with PMT and its predecessor, MediaSentry Inc., since June 2004. MediaSentry provided a suite of anti-piracy services, which included data collection for litigation.

I have been in the computer programming industry for about 14 years. My area of expertise is programming networked applications. Specifically, I work on developing software applications which are designed to communicate with one another over computer networks and the Internet. I have been working directly in the data collection for anti-piracy services field for over 6 years. In addition, I have been attending college since 1998, studying Information Technology, and specializing in data communications and networking. I currently hold an associates and bachelor's degree in IT, and am nearing completion of a master's degree.

At MediaSentry, I personally developed software applications to collect evidence of copyright infringement occurring over the Internet so that evidence could be used in litigation. I have testified as a percipient witness in depositions and trials in two cases regarding these data collection practices and procedures, *Capital Records Inc. v. Thomas-Rasset*, Case No. 06-1497 (MJD/RLE) (D. Minn.) and *Sony BMG Music Entertainment v. Tenenbaum*, Case No. 07cv11446-NG (D. Mass.)

MediaSentry provided the plaintiffs with evidence regarding the downloading of numerous files containing sound recordings from the Gnutella network. All of these files were downloaded over the Gnutella network, from the computers of users based within the United States who were utilizing the LimeWire client application. I further describe the downloading process herein, as well as the log files that MediaSentry recorded that detailed information regarding, among other things, how and when the files were downloaded, and the Internet Protocol ("IP") address from which they were downloaded.

Peer Media Technologies is being compensated at an hourly rate of $170 per hour plus travel and expenses for our services related to this matter.

Download Process

The MediaSentry download process related to this matter took place between 2004 and 2008. This is how it worked. MediaSentry, using publicly available, off the shelf software, searched the Gnutella network for Plaintiffs' sound recordings available for downloading from U.S.-based LimeWire users. When the software found a file that matched the sound recording, the software automatically recorded the Internet Protocol ("IP") address of the user with the file. The software then started another process to download the file with the sound recording and to collect evidence verifying that download. This process then connected to the user directly and requested a "directory browse," which is a listing of the users' file names and associated

metadata in the users' directory of files for sharing. The user's computer then would transmit "data packets," which the software recorded in a log file named "RequestLog.txt". From these data packets, the software would analyze the files that the LimeWire user had in their directory for downloading. The software then automatically selected a subset of those files to download, and then downloaded the files directly from that user. The data packets received from the user were recorded in a log file named "DownloadLog.txt".

Download Data

The MediaSentry software recorded packets of data regarding the downloads described above in a log file named "DownloadLog.txt". This file shows the raw data packets received from the user, containing both (1) the sound recording file and (2) data packet information. The data packet information included the following information relating to the corresponding sound recording file:

- Date time: Each packet header has a timestamp (in EST) recorded by MediaSentry. In addition each packet also contains a "Date:" tag which is in GMT and was transmitted to MediaSentry from the LimeWire user.

- Each packet header has the both the IP address of the source, "Packet Source:", and the destination computers, "Packet Destination:". This shows the source of download, as well as the destination. The destination IP address (MediaSentry computer) has been redacted.

- The received handshake packets show the client application which the source user was running. This is displayed in the "Server:" tag. These tags show that the source users were running the LimeWire client.

- The size of the downloaded file is displayed in the "Content-Range:" tag.

- The name of the file being downloaded (as the source user has it named) is displayed in the "Content-Disposition:" tag, in the "filename=" section. The file hash is displayed in the "X-Gnutella-Content-URN:" tag, typically shown in SHA-1 format.

Verification Process

Once the data collection process was completed, a manual review of all downloaded sound recordings was performed within MediaSentry before providing the data to the plaintiffs. The MediaSentry team would attempt to play the sound recordings to ensure they were playable files, and reviewed all the data collected. The data was then provided to the plaintiffs.

September 30th, 2010

Chris Connelly