

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON

TANYA ANDERSEN, individually and on behalf of all others similarly situated.

Plaintiff

v.

ATLANTIC RECORDING CORPORATION, a Delaware corporation; PRIORITY RECORDS, LLC, a California limited liability company; CAPITOL RECORDS, INC., a Delaware corporation; UMG RECORDINGS, INC., a Delaware corporation; and BMG MUSIC, a New York general partnership; RECORDING INDUSTRY ASSOCIATION OF AMERICA; SAFENET, INC., f/k/a MEDIA SENTRY, INC., a Delaware corporation; SETTLEMENT SUPPORT CENTER, LLC, a Washington limited liability company

Defendants.

No. CV 07-934 BR

**DECLARATION OF
CHRISTOPHER CONNELLY**

I, Christopher Connelly pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am Manager I for the MediaSentry Business Unit of MediaDefender, Inc.

("MediaSentry"). I have personal knowledge of all of the matters discussed in this Declaration.

2. The Recording Industry Association of America ("RIAA"), on behalf of the recording companies that constitute its membership, retained MediaSentry (a) to search peer-to-peer ("P2P") networks to help locate the many individuals who are known to use P2P networks to download and distribute unauthorized copies of sound recordings and (b) to document that those unauthorized copies were contained on, and distributed from, the computers located as a result of that search. To perform this task, MediaSentry used the same search processes that are used by anyone accessing those networks for the purpose of obtaining unauthorized files of

sound recordings. When MediaSentry found such a file and downloaded it, as part of that downloading process, MediaSentry, like any other peer-to-peer user, would receive basic information about the user from whom the file was being downloaded. That information would include, among other things, the Internet Protocol (“IP”) address of the user.

3. One of the P2P networks that MediaSentry searched during its work for the RIAA was the FastTrack network. The most popular file sharing application to use the FastTrack network was known as “KaZaA,” but many other applications existed, including the program known as “KazaaLite.” The network no longer exists in the form it did in 2004, when MediaSentry collected the information at issue in this case.

4. P2P services, like the FastTrack network, allow users to connect easily and anonymously with others on the network. A new user first downloads the necessary P2P software. Once the software is installed and launched, the user is connected to other users of the service – typically millions of people at a time – to search for, copy, and distribute copyrighted works stored on other users’ computers. With the installation of the software, the user creates a “shared” folder on his or her computer in which to store the files that the user downloads from the service, which are then available for copying by other users. So, when a user searches for a file on the network, the user is searching the shared folders of the millions of other individuals on the network.

5. “Prompts” appear on the users’ computer screens to facilitate searches for desired songs, movies, or other content. For example, a user may search for “audio files” by artist, song title, album title, or music category (such as “Top 40”). A user who wants recordings by a particular artist simply types the artist’s name in the appropriate search prompt and clicks a

search button. Within seconds, the service searches the indices and returns a list of copies of the desired work that are available to copy.

6. To obtain a copyrighted work, the user clicks on an entry from the list of search results. By doing so, the user then retrieves a perfect digital copy of the desired sound recording from the computers of one or more other users. In a short time, the copying user has a new, permanent audio copy that he or she can listen to or transfer to a digital device as often as desired. Each time a user makes an unauthorized copy, that copy is available on the copying user's computer (and remains available on the computers of the users from whom the copy was made) to be copied and distributed further by others – resulting in an exponentially multiplying (or “viral”) creation and redistribution of perfect digital copies.

7. The present case offers an illustration of how this works. On May 20, 2004, at approximately 7:24 a.m., Eastern Daylight Time, MediaSentry detected an individual with the username “gotenkito@KaZaA” at Internet Protocol (“IP”) address 4.41.209.23, using the KaZaA online file sharing program on the FastTrack file sharing network to distribute copyrighted sound recordings. This individual was actively distributing 1,288 digital audio files—many of them copyrighted sound recordings—from a “shared” folder on the computer connected to the Internet at IP address 4.41.209.23 to millions of other users of the file-sharing network.

8. Exhibit 1 is a screenshot showing the contents of “Gotenkito’s” KaZaA shared folder, which “Gotenkito,” by connecting a computer to the KaZaA network, specifically authorized all other users of the KaZaA network to view and to request copies from. MediaSentry did nothing, and could do nothing, to alter the information contained in “Gotenkito’s” shared folder. The KaZaA network permitted queries and copying, but did not

permit users to manipulate or change in any way the contents of another user's shared folder, and did not grant users access to any files on a computer other than the shared folder.

9. MediaSentry then initiated the process of downloading each of the 1,288 digital audio files in "Gotenkito's" shared folder to verify that the files actually existed on "Gotenkito's" hard drive. Through this process, the computer connected to the Internet at IP address 4.41.209.23 sent MediaSentry packets of information containing metadata for each of the 1,288 digital audio files in the shared folder. A printout of that metadata is shown in the User Log attached hereto as Exhibit 2. The User Log is a text file showing the contents of "Gotenkito's" shared directory, including all 1,288 digital audio files in this case, and the metadata associated with those files, including the name of each file, the artist, the album, the size of the file, the quality of the file, and any comments about the file. Sound recordings and compact discs sold legitimately in retail stores or online do not include metadata like the comments and keywords found in the attached User Log.

10. MediaSentry then downloaded eleven actual sound recordings (out of the 1,288 available) from the computer on which the songs were stored. To do this, MediaSentry simply requested a copy of these eleven files. The computer on which the files were located then responded by making a copy of each of the eleven digital audio files and transmitting those copies to MediaSentry. MediaSentry monitored the transfer and recorded the IP address of the computer from which the transfer occurred. This address, 4.41.209.23, appears on the download log file that MediaSentry preserved, and which is attached to this declaration as Exhibit 3. The packets of computer data received by MediaSentry are marked "RECEIVED PACKETS" and show, among other things, the date and time the packet was received by MediaSentry, the

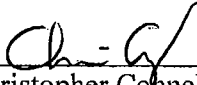
“source” IP address from which the packet was received (in this case, 4.41.209.23), the KaZaA username, the title of the sound recording, and the artist.

11. A printout confirming the actual transfer of these eleven sound recordings to MediaSentry is shown in the System Log attached hereto as Exhibit 4. This document is a record of the downloading process, showing the sound recordings that were downloaded, the time each download was initiated, the time each download was completed, and the “handshake” acknowledgments between MediaSentry’s computer and the computer connected to the Internet at IP address 4.41.209.23. A “handshake” is a term used to describe the process of one computer establishing a connection with another computer or device using standard communication protocols.

12. Using publicly available information regarding the assignment of IP addresses on Arin.net, MediaSentry determined that Verizon Internet Services, Inc. was the Internet Service Provider that had assigned IP address 4.41.209.23 to one of its subscribers on May 20, 2004.

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

Executed this ___8th___ day of May, 2009.



Christopher Connelly