

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

---

CAPITOL RECORDS, INC. et al.,  
Plaintiffs,  
v.  
NOOR ALAUJAN,  
Defendant.

---

Civ. Act. No. 03-cv-11661-NG  
(LEAD DOCKET NUMBER)

---

SONY BMG MUSIC ENTERTAINMENT  
et al.,  
Plaintiffs,  
v.  
JOEL TENENBAUM,  
Defendants.

---

Civ. Act. No 07-cv-11446-NG  
(ORIGINAL DOCKET NUMBER)

**DECLARATION OF ELIZABETH HARDWICK**

I, Elizabeth Hardwick, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Product Manager, Data Services for the MediaSentry Business Unit of Safenet, Inc., formerly MediaSentry, Inc. (“MediaSentry”). I have personal knowledge of all of the matters discussed in this Declaration except as where stated on information and belief. As to such facts, I believe them to be true.

2. MediaSentry is one of the principal providers of online anti-piracy services worldwide. It specializes in providing services to detect and prevent unauthorized distribution of music, films, software, and other content on the Internet.

3. MediaSentry has been engaged by the Recording Industry Association of America (“RIAA”) on behalf of the Plaintiffs to assist them in locating individuals infringing their copyrights over peer-to-peer networks and gathering evidence of their infringement. To perform this task, MediaSentry searches peer-to-peer networks for individuals distributing infringing files for download and gathers evidence concerning that infringement.

4. In gathering evidence of infringement, MediaSentry does not do anything that any user of a peer-to-peer network cannot do and does not obtain any information that is not available to anyone who logs onto a peer-to-peer network. Thus, when MediaSentry searches for sound recordings on the peer-to-peer network, views the files that each peer-to-peer user is disseminating to others, obtains the IP address and screen name of each user, and downloads copyrighted works distributed by each user, it is using functionalities that are built into the peer-to-peer protocols that each user has chosen to use to upload (or distribute) and download (or copy) music.

5. MediaSentry searches peer-to-peer networks, looking for users distributing (“uploading”) files that appear to be digital copies of sound recordings whose copyrights are owned by the RIAA’s member record companies. When MediaSentry finds such a file, it may download the file. As part of that downloading process, MediaSentry, like any other peer-to-peer user, receives basic information about the user from whom the work is being downloaded. That information includes, among other things, the Internet Protocol (“IP”) address of the user.

6. Once connected to the user’s computer MediaSentry also seeks to determine what other files the individual is distributing to others for download. KaZaA and other file-copying programs permit users to share all of the files in their shared folders, and they may contain a feature that permits users to browse the entire shared folder of another user. When available,

MediaSentry invokes this feature of a peer-to-peer program, just as any other user could do, and is able to determine whether the individual user is merely distributing one or two music files or whether the user is distributing hundreds or even thousands of music files.

7. Again using a feature of the peer-to-peer software available to any user, MediaSentry can then capture a list of all of the files that the user is distributing to others for download. MediaSentry collects this information in two forms. First, MediaSentry takes screen shots, which are actual pictures of the screens that MediaSentry or any other user of the peer-to-peer network can see when reviewing the files being distributed. Second, MediaSentry captures as a text file all of the contents of the user's shared directory, such as the names of each file and the size of each file, as well as additional information (called "metadata") about each file. Metadata may include a wide range of information about a file. Metadata, for example, can include information such as identification of the person or group that originally copied the file and began disseminating it unlawfully. MediaSentry does nothing to create this text file; it exists on the user's hard drive and is distributed by the user to anyone to whom the user distributes files.

8. MediaSentry's process for identifying potential infringers and gathering evidence of infringement has multiple fail-safes to ensure that the information gathered is accurate. MediaSentry takes numerous steps to check and double-check the IP address of the potential infringer.

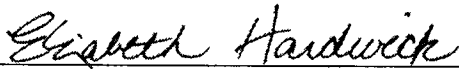
9. MediaSentry followed the procedures outlined above with respect to the evidence that it gathered in this case. Specifically, on August 10, 2004, at approximately 12:49 A.M. EDT, MediaSentry detected the username "sublimeguy14@KaZaA" logged into the KaZaA file-sharing service at IP address 68.227.185.38. Attached as Exhibit B to Plaintiffs' Complaint is a

true and correct copy of a compilation of screen shots captured by MediaSentry on August 10, 2004 showing the list of files that the computer connected to KaZaA with the IP address of 68.227.185.38 was distributing 816 audio files under the username “sublimeguy14@KaZaA” to others for download.

10. Exhibit B indicates that the KaZaA user was “not sharing any files.” This indicated that MediaSentry’s investigator was not sharing any files.

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

Executed this 2nd day of January, 2008.

  
Elizabeth Hardwick