

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X

ATLANTIC RECORDING CORPORATION, et al.,

No. 05 CV 9111 (LTS)(DFE)

Plaintiffs,

-against-

DOES 1-25,

AFFIDAVIT

Defendants.

-----X

STATE OF NEW YORK)
) ss.:
COUNTY OF NEW YORK)

ZI MEI, being duly sworn, deposes and says:

A. Background.

1. I am a web designer, technologist, and internet consultant. A 1999 graduate of Wesleyan University (B.A. Sociology), I have 5 years of web industry experience and over 15 years of computer experience. My areas of expertise span a range of technical and creative aspects, including all facets of web design and development, networking and computer security, database design and programming, GUI design and usability analysis, digital imaging and optimization, game design, print design, and general computer technical support. Among the development tools, languages, and processes in which I am an expert are: Mac and PC operations, Photoshop, ImageReady, Illustrator, Flash, DreamWeaver, Acrobat, HTML, JavaScript, PHP, mySQL, ColdFusion, Access, FileMaker Pro, Microsoft Office, CD-ROM production, web administration, movie and MP3 encoding, peer-to-peer clients, file transfer and storage technologies, and computer

repair. As an early adopter of technological innovation, I have been a computer user and technology enthusiast since age 12. I have been online since circa 1990, before the advent of the World Wide Web, using a 2400 baud modem to connect to local Bulletin Board Systems trading images, DIY documents, short fiction, games, computer utilities, and other shareware. Through my experience as an active member of numerous BBS's, discussion groups, and forums, I have a thorough understanding of the norms, values, and methods of virtual communities in general, and file-sharing communities in particular.

B. Plaintiffs' "Investigation" Is Not Technically Reliable.

2. Annexed hereto as Exhibits "D" and "E", respectively, are the Declaration of Jonathan Whitehead of the Recording Industry Association of America, Inc. ("RIAA") – upon which this Court based its *Ex Parte* Order permitting discovery into the confidential names and addresses of internet service provider customers – and the transcript of the deposition of Gary Millin, the president of MediaSentry Inc., in which he explained in a Canadian litigation the methods used by MediaSentry in conducting investigations for record companies.

3. It is clear from examination of these documents that the methods used by plaintiffs and their agents are not reliable indicators of the existence of copyright infringement on the part of the defendants whose identity plaintiffs seek through this proceeding.

C. Plaintiffs' Infringement Claims Cannot Be Predicated On Metadata

4. Plaintiffs claim that "metadata accompanying each file [allegedly downloaded from defendants' computers by the RIAA] demonstrates that the user is engaged in copyright infringement." Declaration of Jonathan Whitehead (the "Whitehead Declaration"), ¶ 13. No explanation for this assertion is even attempted. This, however, is not surprising since there is no

correlation whatsoever between (a) metadata in the files allegedly downloaded by the RIAA and (b) the origin of these files.

5. Metadata is most commonly defined as “data about data.” Metadata can be associated with various kinds of data formats, including HTML pages, image files, video files, and certain kinds of audio files, including “mp3” files which are the type of files set forth in the lists annexed as Exhibit 1 to the Whitehead Declaration. In the context of mp3 files, metadata refers to the ID3/ID4 tags embedded at the end of the file. These “metatags” provide information comparable to a card catalog in a library, *i.e.*, book title, author, subject matter, publisher and year. A metatag on an mp3 file may also be likened to the sales tag on an article of clothing at a retailer. Such a tag may describe the size, material, care instructions, store inventory control codes, and other information, but *is not an essential part* of the garment and need not be present for the garment to serve its function.

6. In an mp3 file, metatags may indicate the song title, artist, album name, category of music, audio quality, track number, year, etc. Mp3 players can read this information and display it visually. Unlike mp3s, audio CDs do not have ID3/ID4 tags; audio CDs were designed to hold only digital audio data and cannot store auxiliary textual data regarding track names, artists, etc. This is because ID3/ID4 tags did not exist in 1979 when the audio CD format was developed.

7. Mp3 metadata is *optional*. It may or may not be present in a file, and may or may not be accurate. Since metadata is not part of the audio data, a computer or mp3 player can play mp3 files regardless of existence or content of metatags. Moreover, anyone can create, edit or remove ID3/ID4 tags at will through software bundled with MP3 players or any commonly available software program.

8. When a song is first “ripped” (copied) from a CD and encoded on a computer hard drive as an mp3 file, no information about the content of the recording is available. This is because, as noted above, audio CDs were not designed to hold auxiliary textual data about song titles, artists, etc. After the user makes the mp3, he or she may leave the metatags blank, or may enter text data into them manually or by downloading metadata information available online. Exhibit “F” shows how easily anyone can manually change the metadata for an mp3. All one has to do from the Windows platform is select the file, right click on it, go to Properties >> Summary >> Advanced. The user can then input any text into the metatags. As shown in Exhibit “G” hereto, after clicking on “Advanced”, I changed the “genre” metatag of a Metallica song to say “Gangsta Rap”, which is clearly inaccurate since Metallica is a heavy metal band.

9. Metadata is easily changed, and highly prone to intentional tampering, inaccuracies and human error, especially if inputted manually. ID3/ID4 tags and filenames are extremely unreliable, and malicious internet users often change metadata or rename files in an effort to trick other users into downloading Trojans, viruses, or other destructive programs. Among the tactics used by the RIAA and its agents to minimize file-sharing is the placement on the internet of decoy or dummy files which have the *same title and file names* as copyrighted music files. These decoy or dummy files contain segments of an actual song but in the middle may contain noise, static, loops or other audio corruptions. For this reason, one cannot confirm that a file is a true copy of a copyrighted music file or a decoy by listening to only a portion of the file; the only way to make this determination is to listen to the *entire* file, something that plaintiffs do not claim to have done.

10. Simply put, there is no correlation between metadata in a file and the origin of the file. In no way can it be used as a tracking mechanism like a FEDEX or UPS tracking number.

It certainly cannot be used to determine whether the files allegedly found on defendants' computers got there legally or illegally, since those files could have been downloaded from an authorized online service, or copied legally from commercially purchased audio CDs.

D. Plaintiffs' Infringement Claims Cannot Be Predicated On "Matching" Hash Values

11. Furthermore, plaintiffs cannot establish the source of those files by reference to the files' "hash" values. A hash is a compacted message digest consisting of a string of numbers and letters which is used to identify a file and validate its integrity by comparison to the hash value of an original file. (Such validation is useful since a file may become corrupted due to a bad internet connection). As with metadata, hash values cannot be used as a tracking mechanism. A hash value for a particular file may be generated by processing the file through a hashing software program. Such values may be generated for any kind of computer file – text files, images, emails; they are not limited to music files. Among the many different kinds of hash programs is SHA-1 (Secure Hash Algorithm 1). The list of music files annexed as Exhibit 1 to the Whitehead Declaration states an SHA-1 value for each listed file. No explanation is given for the significance, if any, of these SHA-1 values, but they are set forth apparently in an effort to convince the Court that plaintiffs have evidence against defendants, even though they don't.

12. Besides referring to SHA-1 values, the lists contain references to "total matched files" and "total distinct matches." Plaintiffs have not identified the location, source or other identifying characteristics of the files to which plaintiffs supposedly compared the files allegedly on defendants' computers, and thus have not established any "match". Moreover, even if the SHA-1 values of the files were identical, such a "match" would not establish that the files on defendants' computers were obtained through illegal downloading. This is because two completely

separate individuals could create identical SHA-1 values for a music file if they each bought the same audio CD, ripped it onto their separate computers and inputted the same metadata into the ID3/ID4 tags, something which can easily be done by downloading uniform metadata from legitimate online content services such as Gracenote or AMG Lasso. Likewise, if two different users purchased the same mp3 file from the same online music store, the two files would have identical SHA-1 hash values.

E. Plaintiffs Have Not Shown That The IP Addresses Allegedly Linked to Defendants Are Accurate and Authentic

13. Moreover, plaintiffs have not established that the IP addresses, through which the files were allegedly made available, are accurate and authentic. As long as one has already identified a specific IP address, it is relatively simple to determine, by performing a reverse DNS search, the identity of the internet service provider to whom that IP address was assigned. On the other hand, the issue of how plaintiffs first came up with the IP addresses allegedly corresponding to defendants' internet accounts is extremely problematic. As reflected on the Kazaa screenshot printouts that plaintiffs attached as Exhibit 1 to the Whitehead Declaration, the IP addresses of Kazaa users do not appear on Kazaa screenshots and are not displayed to other Kazaa users. The Kazaa software itself offers no means of identifying the IP addresses of Kazaa users. Moreover, IP addresses, which consist of a 12 digit code, can easily be mistranscribed. The exact technical procedures through which the IP addresses in this case were harvested and the technical validity and reliability of those investigative techniques are not explained. Since plaintiffs has not shown how they harvested the IP addresses, it is impossible to discern that these IP addresses were not simply invented.

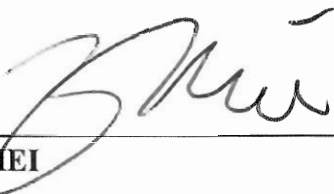
14. In addition, the use by ISPs of dynamic IP addresses further impedes positive identification of internet users. With the exponential growth in the number of new Internet users every year, the world is rapidly running out of IP addresses. One solution is for ISP's to use dynamic IP addresses, assigning subscribers IP addresses on an as-needed basis instead of giving them static IP's. When a user disconnects, his/her IP is released back into the pool. The same IP address may have been assigned to several people over the space of several minutes, depending on turnover rate of users and recycle rate of the ISP's DHCP (dynamic host configuration protocol) server, the machine that assigns IP addresses to users. Dial-up users are always assigned dynamic IP's, as are almost all DSL, cable, and other broadband users.

15. The difficulty of matching a given IP address to an individual with any certitude is further complicated by the fact that an increasing number of users are using wireless routers without using Wired Equivalent Privacy ("WEP"). An overwhelmingly large number of users have WEP disabled, which is the default setting on many, if not, most routers. Most users do not understand enough about networking to know why they need it, or how to turn it on. Others find WEP inconvenient since it requires entering a long password. The result is that numerous devices can be used to "sniff out" open WI-FI access points, including the Nintendo DS and PlayStation Portable handheld gaming systems. Anyone with a wireless device within range can get onto an unprotected wireless network: a next door neighbor, someone sitting in a car outside one's house with a wireless laptop, etc.

16. Even wireless router users who use WEP may still leave themselves significantly exposed if they use the default factory setting as the password (user: admin, password:

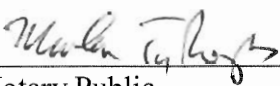
password), or use an easily-guessed password. Once penetrated, an intruder has complete control of the user's network without the router owner even knowing it.

17. Based on the foregoing, plaintiffs' "investigation" of alleged copyright infringement is inherently unreliable and unscientific, and does not form an appropriate basis for invading the privacy of internet users.



ZI MEI

Sworn to before me this
28th day of December, 2005



Notary Public

MORLAN TY ROGERS
Notary Public, State of New York
NO. 02RO6116188
Qualified in Queens County
Commission Expires September 20, 20⁰⁸