

Exhibit A

1. I am Vice President, Anti-Piracy Legal Affairs for the Recording Industry Association of America, Inc. ("RIAA"), where I have been employed for over six years. My office is located at 1025 F Street, N.W., 10th Floor, Washington, DC 20004. I submit this Declaration in support of Plaintiffs' *Ex Parte* Application for Leave to Take Immediate Discovery.

2. As Vice President, Anti-Piracy Legal Affairs, I am responsible for evaluating and contributing to online strategies for the RIAA, including oversight of the investigations into online infringement of copyrighted sound recordings. As such, this Declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

The RIAA's Role in Protecting Its Member Recording Industry Companies From Copyright Infringement

3. The RIAA is a not-for-profit trade association whose member record companies create, manufacture, and/or distribute approximately ninety percent of all legitimate sound recordings produced and sold in the United States. The RIAA's member record companies comprise the most vibrant national music industry in the world. A critical part of the RIAA's mission is to assist its member companies in protecting their intellectual property in the United States and in fighting against online and other forms of piracy. All of the Plaintiffs in this action are members of the RIAA.

4. As part of that process, the RIAA, on behalf of its members, retains a variety of services from outside vendors to assist with its investigation of the unauthorized reproduction and distribution of copyrighted sound recordings online.

The Internet and Music Piracy

5. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to communicate freely and easily and to exchange ideas and information, including academic research, literary works, financial data, music, movies, graphics, and an unending and ever-changing array of other data. Unfortunately, the Internet also has afforded opportunities for the wide-scale piracy of copyrighted sound recordings and musical compositions. Once a sound recording has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in sound quality.

6. Much of the unlawful distribution of copyrighted sound recordings over the Internet occurs via "peer-to-peer" ("P2P") file copying networks or so-called online media distribution systems. The most notorious example of such a system was Napster, which was enjoined by a federal court. Notwithstanding the court's decision enjoining Napster, similar online media distribution systems emerged and attempted to capitalize on the growing illegal market that Napster fostered. These include KaZaA, eDonkey, iMesh, Ares, BitTorrent, DirectConnect, and Gnutella, among others. To this day, some P2P networks continue to operate and to facilitate widespread copyright piracy. At any given moment, millions of people illegally use online media distribution systems to upload or download copyrighted material.

7. P2P networks, at least in their most popular form, refer to computer systems or processes that enable Internet users to: (1) make files (including audio recordings) stored on a computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet. P2P networks enable users who otherwise would have no connection with, or

knowledge of, each other to offer to each other for distribution and copying files off of their personal computers, to provide a sophisticated search mechanism by which users can locate these files for downloading, and to provide a means of effecting downloads.

8. The major record companies generally have not authorized their copyrighted sound recordings to be copied or distributed in unsecured formats by means of P2P networks. Thus, the vast majority of the content that is copied and distributed on P2P networks is unauthorized by the copyright owner – that is, the distribution violates the copyright laws.

9. The scope of online piracy of copyrighted works cannot be underestimated. The RIAA member companies lose significant revenues on an annual basis due to the millions of unauthorized downloads and uploads of well-known recordings that are distributed on P2P networks by infringers who, in virtually all cases, have the ability to maintain their anonymity to all but the Internet Service Provider (“ISP”) they use to supply them with access to the Internet.

10. The persons who commit infringements by using the P2P networks are, by and large, anonymous to Plaintiffs. A person who logs on to a P2P network is free to use any alias (or computer name) whatsoever, without revealing his or her true identity to other users. Thus, Plaintiffs can observe the infringement occurring on the Internet, but do not know the true names or mailing addresses of those individuals who are committing the infringement.

The RIAA’s Identification of Copyright Infringers

11. In order to assist its members in combating copyright piracy, the RIAA retained a third-party investigator, MediaSentry, Inc. (“MediaSentry”), to conduct searches of the Internet, as well as file-copying services, for infringing copies of sound recordings whose copyrights are owned by RIAA members. A search can be as simple as logging onto a P2P network and examining what files are being offered by others logged onto the network. In

gathering evidence of copyright infringement, MediaSentry uses the same functionalities that are built into P2P programs that any user of the software can use on the network.

12. Users of P2P networks who distribute files over a network can be identified by using Internet Protocol ("IP") addresses because the unique IP address of the computer offering the files for distribution can be captured by another user during a search or a file transfer. Users of P2P networks can be identified by their IP addresses because each computer or network device (such as a router) that connects to a P2P network must have a unique IP address within the Internet to deliver files from one computer or network device to another. Two computers cannot effectively function if they are connected to the Internet with the same IP address at the same time. This is analogous to the telephone system where each location has a unique number. For example, in a particular home, there may be three or four different telephones, but only one call can be placed at a time to or from that home. Each computer or network device is connected to a network that is administered by an organization like a business, ISP, college, or university. Each network, in turn, is analogous to an area code. The network provider maintains a log of IP address allocations. An IP address can be associated with an organization such as an ISP, business, college, or university, and that organization can identify the P2P network user associated with the specified IP address.

13. MediaSentry finds individuals using P2P networks to share music files over the Internet. Just as any other user on the same P2P networks as these individuals would be able to do, MediaSentry is able to detect the infringement of copyrighted works and identify the users' IP addresses because the P2P software being used by those individuals has file-sharing features enabled.

14. For each suspected infringer, MediaSentry downloads a number of the music files that the individual is offering to other users on the P2P network. Those music files for each such individual are listed in Exhibit A to the Complaint. MediaSentry assigns an identification number to each individual for which it detects copyright infringement and gathers additional evidence for each individual, such as metadata accompanying each file being disseminated that demonstrates that the user is engaged in copyright infringement. That evidence includes download data files that show for each music file the source IP address, user logs that include a complete listing of all files in the individual's share folder at the time, and additional data that track the movement of the files through the Internet.

15. After MediaSentry collects the evidence of infringement, the RIAA engages in a painstaking process to verify whether each individual was infringing. That process relies on human review of evidence supporting the allegation of infringement. For each suspected infringer, the RIAA reviews a listing of the music files that the user has offered for download by others from his or her computer in order to determine whether they appear to be copyrighted sound recordings. The RIAA also listens to the downloaded music files from these users in order to confirm that they are, indeed, illegal copies of sound recordings whose copyrights are owned by RIAA members. Exhibit A to the Complaint lists the details of these downloaded music files. In my role as Vice President, Anti-Piracy, I provide oversight over the review of the lists contained in Exhibit A to the Complaint and hereby attest to the veracity of those lists. The RIAA also reviews the other evidence collected by MediaSentry.

The Subpoena Process to Identify Copyright Infringers

16. The RIAA frequently has used the subpoena processes of Federal Rule of Civil Procedure 45 and the Digital Millennium Copyright Act ("DMCA") to obtain the names of infringers from ISPs. The RIAA typically has included in their subpoenas to ISPs an IP address

and a date and time on which the RIAA, through its agent, MediaSentry, observed use of the IP address in connection with allegedly infringing activity. In some instances, providing the IP address alone to the ISP has been enough to enable the ISP to identify the infringer. Providing the date and time further assists some ISPs in identifying infringers, especially ISPs that use “dynamic IP addressing” such that a single computer may be assigned different IP addresses at different times, including, for example, each time it logs into the Internet.¹ Once provided with the IP address, plus the date and time of the infringing activity, the infringer’s ISP quickly and easily can identify the computer from which the infringement occurred (and the name and address of the subscriber that controls that computer), sometimes within a matter of minutes.

17. Since 1998, the RIAA and others have used subpoenas thousands of times to learn the names, addresses, telephone numbers, and e-mail addresses of infringers for the purpose of bringing legal actions against those infringers. During a recent litigation with Verizon (an ISP) relating to the DMCA subpoena process, Verizon conceded that, as an alternative to the DMCA process, Plaintiffs could file “Doe” lawsuits and issue Rule 45 subpoenas to ISPs to obtain the true identities of infringing subscribers.

The RIAA’s Identification of the Infringers in This Case

18. In the ordinary course of investigating online copyright infringement, the RIAA became aware that Defendants were offering files for download on various P2P networks. The user-defined author and title of the files offered for download by each Defendant suggested that many were copyrighted sound recordings being disseminated without the authorization of the copyright owners. The RIAA downloaded and listened to a representative sample of the music files being offered for download by each Defendant and was able to confirm that the files

¹ ISPs own or are assigned certain blocks or ranges of IP addresses. An ISP assigns a particular IP address in its block or range to a subscriber when that subscriber goes “online.”

each Defendant was offering for distribution were illegal copies of sound recordings whose copyrights are owned by RIAA members. The RIAA also recorded the time and date at which the infringing activity was observed and the IP address assigned to each Defendant at the time. See Complaint Exhibit A. The RIAA could not, however, determine the physical location of the users or their identities. The RIAA could determine that Defendants were all using Columbia University internet service to distribute and make available for distribution the copyrighted files.

19. The RIAA also has collected for each Defendant a list of the files each Defendant has made available for distribution to the public. These lists often show thousands of files, many of which are sound recording (MP3) files that are owned by, or exclusively licensed to, Plaintiffs. Because of the voluminous nature of the lists, and in an effort not to overburden the Court with paper, I have not attached to this Declaration those lists. Such lists will be made available to the Court upon request. Exhibit A to the Complaint includes the username of the infringer if that was available, the identification number assigned by MediaSentry for that Defendant, and the number of audio files that were being shared by Defendant at the time that the RIAA's agent, MediaSentry, observed the infringing activity.

The Importance of Expedited Discovery in This Case

20. Obtaining the identity of copyright infringers on an expedited basis is critical to stopping the piracy of the RIAA members' copyrighted works.

21. First, every day that copyrighted material is disseminated without the authorization of the copyright owner, the copyright owner is economically harmed. Prompt identification of infringers is necessary in order for copyright owners to take quick action to stop unlawful dissemination of their works and minimize their economic losses.

22. Second, infringement often occurs with respect to sound recordings that have not yet been distributed publicly. Such infringement inflicts great harm on the initial

market for new works. New recordings generally earn a significant portion of their revenue when they are first released, and copyright piracy during a recording's pre-release or early release period therefore deprives copyright owners of an important opportunity to reap the benefits of their labor.

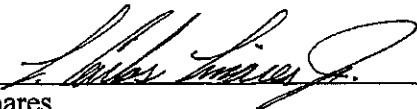
23. Third, without expedited discovery, Plaintiffs have no way of serving Defendants with the complaint and summons in this case. Plaintiffs do not have Defendants' names or addresses, nor do they have an e-mail address for Defendants.

24. Fourth, and perhaps most critically, ISPs have different policies pertaining to the length of time they preserve "logs" which identify their users. ISPs keep log files of their user activities for only limited periods of time – which can range from as short as a few days, to a few months – before erasing the data they contain. If an ISP does not respond expeditiously to a discovery request, the identification information in the ISP's logs may be erased, making it impossible for the ISP to determine the identity of the infringer and eliminating the copyright owner's ability to take action to stop the infringement.

[Remainder of page intentionally left blank.]

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

Executed on March 21, 2008 in Washington, D.C.



Carlos Linares