

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

IN RE: )  
)  
)  
VERIZON INTERNET SERVICES, INC. )  
Subpoena Enforcement Matter )  
\_\_\_\_\_)  
)  
RECORDING INDUSTRY )  
ASSOCIATION OF AMERICA )  
)  
v. ) Miscellaneous Action  
) Case No. 1:02MS00323  
)  
VERIZON INTERNET SERVICES, INC. )  
\_\_\_\_\_)

**Declaration of Frank Creighton in Support of Motion to Enforce July 24 Subpoena Issued  
by This Court To Verizon Internet Services, Inc.**

I, Frank Creighton, have personal knowledge of the facts stated below and, under penalty of perjury, hereby declare:

1. I am Executive Vice President and Director of Anti-Piracy for the Recording Industry Association of America (“RIAA”), where I have been employed for over 17 years. I submit this declaration in support of RIAA’s Motion to Enforce the July 24, 2002 Subpoena Issued By This Court To Verizon Internet Services, Inc.

2. 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.

**RIAA’s Role In Protecting Its Member Recording Industry Companies  
From Copyright Infringement**

3. 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 sold in the United States. A critical part of RIAA's mission is to assist member companies in protecting their intellectual property in the United States, and fighting against online and other forms of piracy.

4. The RIAA Anti-Piracy Unit, which I supervise, investigates the unauthorized duplication and distribution of copyrighted sound recordings of every type. As Executive Vice President and Director of Anti-Piracy, I am responsible for administering and overseeing all domestic investigations into the piracy of copyrighted sound recordings of all kinds, including over the Internet.

### **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 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" file copying. The most notorious example to date has been

Napster, which is now subject to a federal court preliminary injunction. Nonetheless, there are many other peer-to-peer file copying services, including KaZaA, the service used by the alleged infringer in this case, that similarly facilitate wide-spread copyright piracy. Litigation against KaZaA and Grokster – both file copying services – is continuing.

7. “Peer-to-peer” file copying, at least in its most popular form, refers to a computer system or process that enables an Internet user to: (1) make media files (including audio recordings) stored on a computer available for copying by other users; (2) search for media files stored on other users’ computers; and (3) transfer exact copies of the contents of other users’ media files from one computer to another via the Internet. Both Napster’s and KaZaA’s systems 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 PCs; provide as sophisticated a search mechanism by which users can locate these files for downloading; and provide a means of effecting downloads.

8. The major record companies have generally not authorized their sound recordings to be reproduced and distributed in unsecured formats by means of peer-to-peer file copying, or indeed, any other process. Thus, the vast majority of the content that is distributed on peer-to-peer networks such as Napster is unauthorized by the copyright owner – that is, it violates the copyright laws. In the Napster case for example, the Court found, based on a study conducted by RIAA, that at least 87% of the content exchanged on Napster’s service was infringing.

9. The scope of online piracy of copyrighted works cannot be underestimated. Billions of dollars of RIAA's member companies' are lost on an annual basis due to the millions of downloads of well-known recordings that are made available on the Internet by infringers who have the ability to maintain their anonymity to all but the Internet Service Provider ("ISP") they use to supply access to the Internet.

### **RIAA's Historical Use of the DMCA Subpoena And Identification of Infringers**

10. Since 1998, upon the enactment of the Digital Millennium Copyright Act, RIAA has utilized the subpoena provision of this statute approximately 94 times to obtain the identities of alleged infringers of copyrighted sound recordings on the Internet. RIAA began using the provision in specific cases shortly after the statute was passed in 1998. Up until the time of Verizon's refusal in this case, no service provider had ever refused to comply with a DMCA subpoena, except where the provider had destroyed the relevant information and could not provide it. Thus, in virtually all cases, service providers have complied with the subpoenas, and supplied the name, address, and telephone number of the persons sought.

11. In order to assist its members in combating copyright piracy, RIAA does searches of the Internet, as well as file-sharing services, for infringing copies of sound recordings whose copyrights are owned by RIAA members. These searches generally result in the identification of specific IP (Internet Protocol) addresses from which infringers are making unauthorized copies of media files available to the public. The IP address is a unique identifier that, along with the date and time, specifically identifies a particular computer or server using the Internet.

The IP address also specifically identifies the ISP that the individual is using to access the Internet.

12. At the time RIAA identifies an infringer, it knows only the IP address and the Internet pseudonym that the individual uses. While the IP address does identify the infringer's service provider, it does not tell RIAA, or anyone other than the service provider for that matter, definitively whether the infringing material is stored on the service provider's network or on the infringer's personal home computer. Similarly, the IP address does not allow RIAA to determine whether the infringer is operating from a home, a business, or a university. The only information that RIAA can determine from the IP address is the infringer's service provider. Only the service provider will be able to know, with certainty, whether the infringing material resides on one of its own servers or on an individual's home computer.

13. At no time prior to issuing the subpoena to Verizon had a service provider refused to comply with a subpoena because it determined that the information requested did not reside on its system or network, as Verizon appears to claim here. Indeed, Verizon itself has repeatedly told RIAA that it would provide RIAA with information identifying infringers in response to subpoenas issued under Section 512(h) where the infringing material did not reside on its system or network. Nine different times in 2000, RIAA sent notices to Verizon (or its predecessor, Bell Atlantic Internet Solutions, Inc.) asking Verizon to take down specific infringing material from its network. In each of those instances, Verizon's DMCA contact person, Lauren K. Crowder, informed the RIAA that it could not be required to take down the allegedly infringing material because such material was not on a Verizon Internet server, but instead invited that the RIAA "provide [Verizon] with a written subpoena, pursuant to 17 U.S.C. § 512(h), if you would like

for us to provide you with identification information about this user. Upon receipt of the subpoena, we will disclose to you the information requested, subject to the provisions of Section 512(h).” Copies of these letters are attached to this Declaration as Attachment A.

14. Obtaining information via the DMCA’s “expeditious” subpoena process is critical to stopping the piracy of RIAA members’ copyrighted works. The subpoena provision enables RIAA to preserve evidence that the RIAA may need in pursuing actions against infringers. Speed is of the essence for three reasons. First, every day that copyrighted material is disseminated without the authorization of the copyright owner, the copyright owner is economically harmed. Second, service providers have different policies pertaining to the length of time they preserve “logs” which identify their users. If a service provider does not respond expeditiously to the subpoena request, the identification information in the service provider’s logs may be destroyed, making it impossible to determine the identity of the infringer. Third, time is most critical in the context of widespread dissemination of a sound recording *prior* to the recording ever being distributed publicly. In these pre-release settings, it is critical that RIAA be able to respond quickly so that the artists who create the sound recordings have a fair chance to reap the benefit of their labor.

15. Upon receiving information about the infringer from a service provider, RIAA has several options, which depend on a variety of circumstances. In some cases, it will be sufficient that the service provider will have complied with a request from RIAA to either take down or disable access to the infringing material. In others, where the infringer is a repeat offender, RIAA may inform the service provider that it should implement the “repeat infringer” policy that it is required to have under the DMCA. In many cases, RIAA may send a “cease and desist”

letter to the now -identified infringer. This is especially important in a case where the service provider does not disable access to the infringing material; only by seeking recourse from the individual infringer can the copyright owner stop the ongoing infringement of its copyrights. Finally, RIAA has the option of suing the individual identified in order to protect its member companies' copyrighted works or referring the case for criminal prosecution.

### **RIAA's Identification of The Infringer & Issuance of the DMCA Subpoena In This Case**

16. In this case, RIAA did not use an automated system to identify the IP address specified in the July 24 subpoena. To the extent that Verizon and *amicis* suggest otherwise, that is simply false. Instead, an RIAA employee on my staff conducted manual searches, by searching for the name of one of its members' recording artists. After finding a file that claimed to contain that artist's recording, the RIAA employee conducted a download of that file to his or her own computer. While this download was being conducted, the RIAA employee used a computer program to identify where the download was coming from, i.e., the IP address of the computer or server which maintained the infringing material and the associated ISP that has been assigned that IP address.

17. Once the IP address is identified, some file -copying services, such as KaZaA, give users the opportunity to view other files being offered by the same user. Thus, once the IP address is associated with the pseudonym the infringer uses on KaZaA, a user can view all of the other sound recordings that the infringer has chosen to make available. Those additional files can then be downloaded from the same IP address.

18. That is exactly what occurred in this case. The RIAA employee obtained a listing of the files that the individual infringer had made available to all KaZaA users. Each of the files was identified by the name of a sound recording, often a popular song, the name of the artist, or a combination of both. Those artists included Billie Holiday, the Beatles, the Who, Pete Seeger, James Taylor, Bob Marley, Johnny Cash, Stevie Wonder, Billy Joel, Barry White, Aerosmith, Janet Jackson, Madonna, U2, Jennifer Lopez, N' Sync, Britney Spears, and countless others. All told, there were over 600 sound recordings listed that were available for download. Almost all were sound recordings whose copyrights were owned or controlled by RIAA members.

19. The RIAA employee downloaded and listened to a sample of the works listed, and confirmed that the infringing material were actual copies of the copyrighted recordings. Attached as Attachment B are sample screenshots showing the downloads of the infringing works in progress.

20. Based on all of this information, RIAA sought and obtained a DMCA subpoena from the Clerk of the District Court to uncover the identity of this significant infringer. RIAA provided to Verizon information, including the IP address, as well as the date and time the files were made available from this IP address. This information would allow Verizon to specifically identify the individual infringer. RIAA also provided the list of infringing sound recordings that were available for download. At the time it obtained the July 24, 2002 subpoena from this Court, RIAA did not definitively know (indeed could not know) whether the offending files obtained via the IP address that it identified resided on Verizon's network or on an individual's computer. In fact, RIAA has still not been able to independently verify whether the infringing sound recordings reside on Verizon's network.

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

Dated: September 4, 2002

---

Frank Creighton