



August 14, 2003

Hand Delivered

Senator Norm Coleman
Chairman
Permanent Subcommittee on Investigations
Committee on Governmental Affairs
United States Senate
Russell Senate Office Building, Room 199
Washington, DC 20510-6250

Dear Mr. Chairman:

Thank you for the opportunity to respond to your letter of July 31, 2003, and to provide information regarding the recording industry's current efforts to fight online music piracy. As you know, the Recording Industry Association of America ("RIAA") is the trade association representing the United States recording industry. RIAA members, comprised of hundreds of record labels, create, manufacture and/or distribute approximately 90 percent of all sound recordings legitimately sold in the United States. We understand that you have questions regarding RIAA's announcement on June 25, 2003, to collect evidence against individual computer users who are illegally offering for copying substantial amounts of copyrighted music over peer-to-peer networks. RIAA welcomes this occasion to explain our efforts to combat the devastating effects that the massive illegal copying on peer-to-peer networks is having on the music industry. The problems currently facing the music industry will, as broadband expands, soon be the problems of all copyright holders. This is a point of national importance, as the copyright industries constitute five percent of the Gross Domestic Product and copyrighted works are the single largest United States export.

Before turning to your questions, we wish to provide some background information, because our actions are not occurring in a vacuum and are the product of much deliberation. The decision to enforce our rights against egregious infringers was taken only after suffering years of mounting harm. The music industry first tried to use an aggressive public education campaign to discourage the unauthorized distribution of recordings, by explaining to the public that online piracy is not only illegal, but robs songwriters and recording artists of their livelihoods, stifles the careers of up-and-coming musicians, and threatens the jobs of tens of thousands of less celebrated people in the music industry. The music industry also pursued lawsuits against the

Chairman Coleman
August 14, 2003
Page 2 of 11

peer-to-peer systems, which are knowingly facilitating the illegal distribution of copyrighted recordings on a massive scale. Most important, the music industry has aggressively licensed legitimate online music services to offer legal alternatives to consumers. Only after these steps did not stem the tidal wave of illegal conduct has RIAA resorted to its current course, pursuing the users of peer-to-peer networks who are distributing substantial amounts of unauthorized copies of recordings. And there is one point on which all of the courts have agreed: these users are violating the copyright laws. Our heightened enforcement efforts are deliberately occurring now; when, as a result of the music industry's extensive educational efforts, the public is more aware than ever before of the illegality and consequences of online piracy and, at the same time, the number of legitimate online music sources is exploding, giving music lovers a multitude of options for legally obtaining music online.

The Piracy Problem Facing the Music Industry

In the past three years, shipments of recorded music in the United States have fallen by an astounding 26 percent, from 1.16 billion units in 1999 to 860 million units in 2002. And worldwide, the recording industry has shrunk from a \$40 billion industry in 2000 down to a \$32 billion industry in 2002. Hit records – which are critical to the long-term health of the music industry and enable investment in new artists and new music – have suffered most dramatically. In 2000, the ten top-selling albums in the United States sold a total of 60 million units. In 2001, that number dropped to 40 million. Last year, it totaled just 34 million.

The root cause for this drastic decline in record sales is the astronomical rate of music piracy on the Internet. Computer users illegally download more than 2.6 billion copyrighted files (mostly recordings) every month. At any given moment, well over five million users are online offering well over 1 billion files for copying through various peer-to-peer networks. Peer-to-peer networks allow a user to make media files, including recordings, stored on that user's computer available for copying by others; to search for media files stored on other users' computers; and to transfer exact copies of the contents of other users' media files to that user's own computer. A song can be copied and distributed in this manner an unlimited number of times, without any degradation in sound quality. And unlike traditional music piracy, piracy through networks is viral: unless the user takes affirmative steps to prevent it, the user automatically and immediately begins offering the files that the user copied to millions of other users. Moreover, the overwhelming majority of the distribution that occurs on peer-to-peer networks is unauthorized.

It is widely recognized and acknowledged that individuals who engage in such unauthorized distribution – either by making recordings available for others to copy or by making copies of others' files – are committing a clear violation of the copyright laws. The courts have been unanimous on this point. As the Ninth Circuit explained in the *Napster* case, “a majority of Napster users use the service to download and upload copyrighted music. . . . And by doing that, . . . the uses constitute direct infringement of plaintiffs' musical compositions, recordings.” Judge Wilson quoted this language in the recent *Grokster* case, and similarly recognized that many Grokster and Streamcast users were downloading copyrighted music, “thereby infring[ing] [copyright owners'] rights of reproduction and distribution.” Most

Chairman Coleman
August 14, 2003
Page 3 of 11

recently, in a case involving Aimster, Judge Posner of the Seventh Circuit noted that Aimster users who were distributing or making copies of copyrighted music were copyright infringers, and that there was no evidence in the record before him that Aimster "has ever been used for a noninfringing use."

According to a November 2002 survey by Peter D. Hart Research, by a nearly 2-to-1 margin, consumers who say they are illegally downloading more music report that they are purchasing less music. The same survey found that the main reason consumers are not buying more music is that they get a lot of what they want for free by illegally downloading or copying it from others. In a similar study conducted in May 2002 by Peter D. Hart Research, among 12- to 18-year-olds, 35 percent say the first thing they will do after hearing a new song that they like is download it, versus just 10 percent who will buy it. Among 19- to 24-year-olds, 32 percent download the new song first, versus 9 percent who will buy it.

These findings are bolstered by a June 2003 Edison Media Research report which found that "among the heaviest downloaders, 48% say they no longer have to buy CDs because they could download music for free over the Internet" – an increase of 61 percent in just one year. It is thus not surprising that, while sales of music CDs are dropping, sales of blank CDs (onto which downloaded recordings can be copied) have increased dramatically, by more than 30 percent in 2002. Sales of blank CDs now outstrip sales of music CDs by a more than 2-to-1 margin.

These findings are consistent with the skyrocketing number of users of peer-to-peer networks. As of July 2002, Kazaa – the most popular peer-to-peer network by far – boasted 100 million registered users. By May 2003, Kazaa had become the world's most downloaded software program of any kind, with 230.3 million downloads.

Although these peer-to-peer networks are well aware of the rampant illegal copying that occurs over their systems, they have taken no concrete steps to stop it, and in fact, they encourage and enable that conduct, while at the same time taking steps to shield themselves from liability. They provide no meaningful warning to their users that uploading or downloading copyrighted recordings violates the law. They provide no filter to prevent exchange of copyrighted material, even though many provide filters that at least attempt to block pornography and viruses. And the peer-to-peer networks establish "default" settings that, unless affirmatively changed by the user, automatically make the files on the user's hard drive available for copying by anyone else on the network. As Judge Wilson observed in the movie and music industries' case against Grokster, Streamcast, and Kazaa, these peer-to-peer networks "may have intentionally structured their businesses to avoid secondary liability for copyright infringement, while benefiting financially from the illicit draw of their wares." Indeed, Kazaa has established itself in the country of Vanuatu, while the illegal activities on its network are causing the loss of numerous jobs in the music industry in the United States.

Chairman Coleman
August 14, 2003
Page 4 of 11

The Availability of Legal Online Music

The widespread availability of free illegal copies to download through these peer-to-peer networks has greatly interfered with the development of legitimate online sources of music. But music lovers need not break the law to obtain their favorite music online. The music industry continues to respond to consumer demand by making its music available to a wide range of authorized online subscription, streaming, and download services that make it easier than ever for fans to get music legally on the Internet. There are now many legal and inexpensive ways to get music online. In the United States market alone, there are dozens of excellent legitimate online services that offer a variety of choices to enjoy and purchase online music. These services include:

aolmusic.com, apple.com/music, audiocandy.com, bestbuy.com, bet.com, buymusic.com, catsmusic.com, CircuitCity.com, collegeconcerts.com, cornercd.com, dimple.com, dothehole.com, earwax.com, efetus.com, emusic.com, exitosmusical.com, facethemusic.com, fullaudio.com, FYE.com, galleryofsound.com, independentrecord.com, instavid.com, latinoise.com, liquid.com, burnitfirst.com, listen.com, mainstreetmusic.com, millenniummusic.com, miramag.com, mp3.com, mtv.com, musicmatch.com, musicmillennium.com, musicnet.com, musicrebellion.com, netscape.com/music, newworldrecord.com, phillysoulclassics.com, pressplay.com, qhut.com, raspustinmusic.com, real.com/realone/rhapsody, recordandtapetraders.com, rollingstone.com, samgoody.com, spinner.com, streamwaves.com, tophitsmusic.com, towerrecords.com, windowsmedia.com.

Indeed, the number of legitimate online sources of music is continuing to increase. Additional major retailers and software companies – including companies that are household names – plan to enter the online market within the next six months.

The Music Industry's Massive Educational Campaign

The music industry has, for a number of years, undertaken a massive campaign to educate consumers regarding the illegality of the unauthorized distribution of copyrighted music online. Recording industry leaders, along with an unprecedented coalition of other groups like the National Music Publishers' Association, the Country Music Association, the Gospel Music Association, the American Federation of Television and Radio Artists, American Federation of Musicians, ASCAP, BMI, SESAC, the Songwriters Guild of America, Nashville Songwriters Association International, National Association of Recording Merchandisers, and many others, as well as individual songwriters, recording artists, retailers, and record companies have been educating music fans that the epidemic of illegal distribution of music not only robs songwriters and recording artists of their livelihoods, but also undermines the future of music itself by depriving the industry of the resources it needs to find and develop new talent. In addition, it threatens the jobs of tens of thousands of less celebrated people in the music industry, from engineers and technicians to warehouse workers and record store clerks.

Chairman Coleman
August 14, 2003
Page 5 of 11

The message of this campaign has been very clear: copying or distributing copyrighted music over the Internet without permission is stealing, plain and simple. Downloading illegal copies is no different than shoplifting CDs out of a record store, and uploading those recordings for others to illegally copy is no different than handing out stolen CDs on the street corner – and the act of downloading or uploading music on peer-to-peer networks is not an anonymous one. This message has been conveyed to the public in a series of print and broadcast ads featuring more than a hundred major artists and songwriters who ask their fans to stop stealing their music. These ads have appeared in a wide variety of outlets, including USA Today, BET, and MTV. The Grammy award-winning artists participating in this campaign range from country artists Brooks & Dunn and Martina McBride to rock artist Peter Dinklage to Christian artist Steven Curtis Chapman to opera star Luciano Pavarotti to hip hop artists DMX and Missy Elliot to legends Stevie Wonder, Brian Wilson, Don Henley and Elton John, among many others. Other participants include songwriters, session musicians, and retail store owners discussing the impact of music piracy in terms of lost sales, lost jobs, and closed stores.

This antipiracy message is also featured on a music industry website, www.musicunited.org, which contains a number of clips from this educational campaign. The website also includes a wide array of pertinent information, including a description of the governing law, a list of legal online music sources, a guide for parents, as well as step-by-step instructions on how to disable or uninstall peer-to-peer software used to illegally offer music for copying.

Since April 2003, RIAA has been sending Instant Messages – and has now sent well over 4 million – directly to infringers on peer-to-peer networks. These messages inform infringers that their actions are illegal and direct them to the Music United website (www.musicunited.org) for information on how they can avoid breaking the law. While some users are responding to RIAA's messages by ceasing their illegal conduct, others have chosen to react by questioning RIAA's enforcement campaign rather than their own conduct. Kazaa, far from cooperating with this attempt to educate its users about the law, reconfigured the newest version of its software to disable the instant messaging system, thereby preventing RIAA from sending messages to Kazaa's newest users. Kazaa did not, however, change its "default" settings, which, as noted above, automatically make each user's files available for copying by others.

Moreover, prior to beginning our efforts to collect information on substantial infringers, RIAA publicly announced its intent to do so, giving infringers another opportunity to discontinue their illegal conduct. Since that announcement, virtually every major newspaper and television news channel, and hundreds of local news outlets, has covered RIAA's heightened enforcement efforts.

Chairman Coleman
August 14, 2003
Page 6 of 11

The Information Subpoena Provision of the Digital Millennium Copyright Act

As you know, RIAA is collecting evidence pursuant to what is commonly referred to as the information subpoena provision of the Digital Millennium Copyright Act ("DMCA"), which is 17 U.S.C. §512(h). Congress enacted the DMCA in 1998 to encourage development of the Internet's potential, while at the same time protecting against the "massive piracy" of copyrighted works that Internet technology permits. One of the purposes of the DMCA was to allow copyright holders to enforce their copyrights against direct infringers rather than the Internet Service Providers ("ISPs"). Thus, in crafting the DMCA, Congress included a fair and balanced procedure – the information subpoena provision – to ensure that copyright owners, with the help of ISPs, have an accessible and efficient mechanism for identifying individuals who are using the Internet to commit piracy.

The balance struck by Congress in §512 was the result of a give and take – in the best sense – between the interests of ISPs and copyright owners, and the need to protect consumers. Congress recognized that traditional enforcement remedies available to copyright owners were insufficient in an era in which massive amounts of piracy could occur instantly at the hands of anyone with an Internet connection.

ISPs recognized that in a digital world they could have exposure to copyright claims, and thus sought from Congress limitations on liability in the DMCA. ISPs wanted copyright owners to focus on the direct infringers, but recognized that ISPs often would be the sole source for identifying individuals who are engaged in online piracy. So, in exchange for exempting ISPs from any monetary liability for the infringing activities occurring on or over their networks and connections (subject, of course, to certain prerequisites), Congress created a framework by which copyright owners, with the assistance of ISPs, could expeditiously identify individuals engaging in infringing activities online. That compromise – expeditious access for copyright owners to identifying information of infringers, in exchange for broad liability limitations for ISPs – is as fair today as it was in 1998.

It is important to note that absent the broad liability limitations of the DMCA, ISPs would most certainly be liable for secondary copyright infringement for the actions of their subscribers. ISPs who resist DMCA subpoenas are trying to enjoy the safe harbor benefit provided them by the DMCA, without shouldering the minimal corollary burden of responding to subpoenas, which is even less burdensome than would be responding to a notice to remove infringing material from their networks. That fact helps explain why Judge Bates – the federal district judge who presided over the subpoena enforcement proceedings between RIAA and Verizon – concluded as follows: "It would not serve the public interest for Verizon to continue to receive the benefits of the [DMCA] – liability protection – without the concomitant obligations of disclosing the identity of an alleged infringer [under §512]."

To achieve their purpose, DMCA subpoenas must bear fruit quickly. An individual Internet pirate can cause tens of thousands of infringing copies to be distributed in a single day. In the case of recordings that have not yet been released publicly, the economic impact of this

Chairman Coleman
August 14, 2003
Page 7 of 11

viral propagation can be devastating. Thus, as Judge Bates noted, Congress provided "express and repeated direction to make the subpoena process 'expeditious.'"

At the same time, Congress carefully built safeguards into §512 to ensure that it is used only to enforce valid copyright claims. A copyright owner or its agent must supply a "sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title." 17 U.S.C. §512(h)(2)(C). The copyright owner must also file a notification that, among other things, identifies material being infringed and information sufficient to allow the service provider to locate the material and, if appropriate, disable access to it. By substantially complying with this notification requirement, the copyright owner or its agent has established the bona fides of its ownership and claim of infringement.

With this background, our responses to the specific requests for information are as follows:

1. *Copies of all subpoenas issued to Internet Service Providers (ISP) requesting information about subscribers.*

At the request of your Staff Director, Ray Shepherd, we expedited our response to this portion of your request. By letter dated August 8, 2003, RIAA provided to Mr. Shepherd copies of approximately 1075 subpoenas. These comprise all of the DMCA subpoenas that were issued at RIAA's request between June 25, 2003 (the date RIAA announced its heightened efforts to collect evidence against individual computer users who are illegally offering to "share" substantial amounts of copyrighted music over peer-to-peer networks), and the date of your letter. As discussed further below, each subpoena contains a representative list of copyrighted recordings that the individual infringer is illegally distributing, *see* 17 U.S.C. §512(c)(3)(A)(ii), but this list by no means represents the only recordings that the infringer is offering for illegal copying. Indeed, each of these infringers is illegally offering for download a very large number of recordings.

2. *A description of the standard that RIAA is using when filing an application for a subpoena against an ISP with a U.S. District Court.*

When RIAA files an application for a subpoena from a United States District Court, it uses the standard set forth in the information subpoena provision of the DMCA, §512(h). In accordance with that section, RIAA seeks a subpoena only if it can provide the following to the clerk of the federal district court:

- A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive copyright that is allegedly infringed.
- Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

Chairman Coleman
August 14, 2003
Page 8 of 11

- Identification of material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
- A statement that RIAA has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
- A statement that the information in the notification is accurate, and under penalty of perjury, that RIAA is authorized to act on behalf of the owner of an exclusive copyright that is allegedly infringed.
- A sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under the copyright laws.

RIAA recognizes that a failure to adhere to any of these requirements is a justification for denying the subpoena and that any copyright owner who misrepresents itself in satisfying these requirements is potentially liable for damages, including attorney's fees. Thus, as described further below, RIAA takes great care to ensure that a user is illegally distributing or copying copyrighted recordings before it files a request for a subpoena.

Moreover, although the DMCA sets forth the minimum requirements for seeking a subpoena, RIAA is not seeking a subpoena as to everyone who is illegally distributing copyrighted recordings. Rather, at this time, RIAA is focusing on egregious infringers, those who are engaging in substantial amounts of illegal activity. In so prioritizing its efforts, RIAA is acting no differently than anyone in this country whose property rights have been violated and who is faced with a decision whether to press a legal claim: we are making a judgment as to whether pursuing a possible lawsuit is appropriate given the circumstances.

3. *A description of the methodology RIAA is using to secure evidence of potentially illegal file sharing by computer users.*

As discussed above, peer-to-peer networks like FastTrack and Gnutella are, by design and practice, open networks that enable individual users to search for and copy files located on the hard-drives of other users on the network. To gather evidence against individual infringers, RIAA typically uses software that searches the public directories available to any user of a peer-to-peer network. These directories list all the files that other users of the network are currently offering to distribute. By logging onto these open networks and searching for recordings owned by RIAA's members just like any other user, the software finds users who are offering to distribute copyrighted music files. When the software finds such a user, it downloads a sample of the infringing files, along with the date and time it accessed the files, and locates the user's Internet Protocol ("IP") address. Additional information that is publicly available allows RIAA to then identify the infringer's Internet Service Provider.

Chairman Coleman
August 14, 2003
Page 9 of 11

Before acting on any of the information obtained by the software, an employee at RIAA manually reviews and verifies the information. And, before filing a request for a subpoena, RIAA sends the infringer's ISP advance notice that RIAA intends to issue a subpoena with respect to a particular IP address. Among other things, that allows the ISP, if it wishes, to notify its subscriber that its account is soon to be the subject of a subpoena request. Only after completing all of these steps does RIAA request a subpoena from the clerk of court (using the standard set forth in the DMCA as discussed above), seeking from the ISP identifying information for the individual whose account was being used to distribute the copyrighted music.

4. *A description of the privacy safeguards RIAA is using when securing this information in an effort to prevent unfair targeting of de minimis users.*

First, RIAA is in no way targeting "de minimis" users. RIAA is gathering evidence and preparing lawsuits only against individual computer users who are illegally distributing a substantial amount of copyrighted music. As indicated above, the subpoenas issued at the request of RIAA thus far involve infringers distributing very large numbers of copyrighted recordings. By way of example only, we have uncovered infringers with thousands of recordings. That said, RIAA does not condone any illegal copying – and does not want anyone to think that even a little illegal activity is acceptable. Indeed, in the case of a recording that has not yet been released, the illegal distribution of just that one file can have a devastating impact on the sales of the forthcoming album.

While the record companies have not yet filed copyright infringement suits based on the evidence received as a result of the DMCA subpoenas that the RIAA has issued, we assure you that we will approach these suits in a fair and equitable manner. To the extent that infringers are interested in settling those cases, we will discuss settlement on a case-by-case basis, taking into account the individual's particular circumstances. Historically, we have dealt fairly with those who have engaged in online infringement. Last spring, the record companies brought suits against college students who had established and were running unauthorized peer-to-peer networks on their college networks, on which they were illegally distributing tens of thousands of recordings. The industry settled those cases for \$12,500 to \$17,000. While every case is unique, we intend to be similarly fair and proportionate with respect to individual infringers and to consider each individual's circumstances.

Second, as discussed above, the DMCA itself builds in ample safeguards for the privacy of individuals. As Judge Bates held, "These [§512 information subpoena] protections ensure that a service provider will not be forced to disclose its customer's identifying information without a reasonable showing that there has been copyright infringement" and "[t]hese requirements provide substantial protection to service providers and their customers against overly aggressive copyright owners and unwarranted subpoenas." As Judge Bates noted in his decision, the DMCA subpoena process "provide[s] greater threshold protection against issuance of an unsupported subpoena than is available in the context of a John Doe action." This is undoubtedly true.

Chairman Coleman
August 14, 2003
Page 10 of 11

Under the DMCA subpoena process, there are statutory limits on the type of information a copyright owner can obtain via subpoena and the purpose for which that information can be used. Under a DMCA subpoena, a copyright owner can only receive information that is necessary to identify and contact the alleged infringer – such as a name, address, phone number, and e-mail address. More importantly, the copyright owner is statutorily limited to using that information exclusively for purposes of enforcing its copyright. Compare that to filing a “John Doe” lawsuit, in which any aggrieved party could issue a subpoena requesting anything relating to the subscriber account, including user habits, website visits, and payment records. Moreover, once that information has been provided to a copyright owner via a subpoena in the context of a John Doe lawsuit, there are no statutory restrictions whatsoever on how it can be used or with whom it can be shared.

In short, requiring copyright owners to file John Doe lawsuits would provide fewer protections to an ISP’s subscribers, while effectively depriving copyright owners of expeditious access to an alleged infringer’s information. That would defeat the careful balance crafted by Congress in the DMCA. Moreover, a substantial influx of John Doe suits would be much more burdensome on the court system. If RIAA were filing John Doe lawsuits in place of each of these DMCA subpoenas, that would affect not only the clerk’s office but also the judges.

RIAA shares your concern with respect to not overwhelming the court. It thus has worked with the clerk’s office, since prior to beginning our heightened efforts, to establish a process (including providing files electronically) that is acceptable to the court, and has issued its subpoenas on a rolling basis to minimize any impact on the workings of the clerk’s office. Moreover, RIAA is willing – and would very much like – to reduce substantially the number of subpoenas it issues by providing multiple IP addresses for the same ISP on each subpoena. RIAA believes the DMCA allows this practice but, because many of the ISPs have objected, to date the RIAA has issued separate subpoenas for each IP address. Providing multiple addresses per subpoena would significantly reduce the administrative tasks for the clerk’s office, and any support you could provide on this issue would be greatly appreciated.

Third, copyright infringers on peer-to-peer networks should have little expectation of privacy. Individuals on peer-to-peer networks have opened their computers, permitting access to countless others to copy whatever they wish. As Judge Bates observed, “it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world.” The use of peer-to-peer networks is not anonymous: the user’s IP address is publicly available to anyone else on the peer-to-peer network, and the user’s ISP can determine which subscriber was using that IP address. Moreover, almost all ISPs disclose in their User’s Terms of Service that, pursuant to the DMCA, they must provide the subscriber’s identity to a copyright holder when there is reason to believe copyrights are being infringed. For example, Verizon informs its subscribers that it will “disclose individual customer information to an outside entity . . . when Verizon is served with valid legal process for customer information.”

Chairman Coleman
August 14, 2003
Page 11 of 11

Finally, although others may have, RIAA has not been disclosing any information with respect to any infringer, other than the information contained in the subpoena request. The information in the subpoena request, by definition, does not include the identity of the infringer, as that is the very information that RIAA is seeking via the DMCA subpoena.

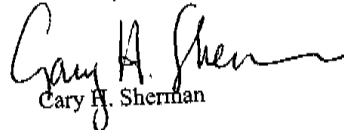
5. *A description of how RIAA is protecting the rights of individuals from erroneous subpoenas.*

RIAA is not aware of any instance in which it has requested a subpoena in the absence of copyright infringement. As explained above, when recordings are offered for distribution on a peer-to-peer network, the user's computer identifies itself with a unique IP address. That address can easily be matched to a particular Internet account and thus it is relatively easy to correctly identify the owner of the Internet account that is being used to offer illegal files. To the extent the subscriber is not the one who is actually participating in the illegal downloading, RIAA cannot know that before it issues the subpoena and, in any event, the subscriber should be monitoring potential illegal uses of his or her Internet account. We suspect that, just as parents would want to know if their children were shoplifting at the local mall, they will want to know if their children are stealing music online. In addition, as noted above, RIAA carefully and manually reviews the information supporting each subpoena request before it makes a request. A request for a subpoena is not made unless the stringent requirements and safeguards of the DMCA, as described above, are met.

Mr. Chairman, I hope this letter fully responds to your inquiry. We at RIAA appreciate your interest in these matters and assure you that we have not taken these steps lightly. No industry likes to be in the position of suing those it hopes to convert to paying customers. But education alone has not worked, and we are faced with a massive problem that threatens not only the industry and everyone who works in it, but the very future of music itself. Just like any retailer who pursues those who shoplift merchandise from their stores, the music industry is simply enforcing its property rights against those who are stealing its music. And our efforts are having an effect. The same day we brought suits against several college students who had set up and were running the unlicensed peer-to-peer systems on their college networks, many other students voluntarily shut down their similar networks on other campuses. We recognize that we cannot eradicate all illegal online copying – just as brick-and-mortar stores cannot prevent all shoplifting – yet we hope to create an environment where legitimate services can and will flourish.

Please do not hesitate to contact me if you have any further questions or concerns.

Sincerely,



Cary H. Sherman