Testimony of

Cary Sherman

September 9, 2003

STATEMENT OF CARY SHERMAN
PRESIDENT AND GENERAL COUNSEL
RECORDING INDUSTRY ASSOCIATION OF AMERICA
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
ON
"PORNOGRAPHY, TECHNOLOGY, AND PROCESS: PROBLEMS AND SOLUTIONS ON PEER-TO-PEER NETWORKS"

SEPTEMBER 9, 2003

Introduction:

Let me begin by thanking Chairman Hatch and the Ranking Member, Senator Leahy for inviting me to testify today and for their ongoing commitment to protecting intellectual property.

My name is Cary Sherman. I am the President of the Recording Industry Association of America, the trade association representing the U.S. recording industry. RIAA members create, manufacture and/or distribute 90 percent of all legitimate sound recordings in the United States.

I'd like to take a minute to give the Committee some information regarding our announcement yesterday that we filed lawsuits against individuals who were sharing hundreds or thousands of copyrighted music files on public peer-to-peer ("P2P") networks. I'd be happy to answer any of the Committee's questions regarding our enforcement efforts.

Turning my attention to the subject of today's hearing, I would like to give the Committee a sense of the gravity of the piracy problem affecting our industry because I think it helps put in context the broader issues being addressed today.

The Piracy Problem Facing the Music Industry:

To date, over the past three years shipments of recorded music in the U.S. have fallen by an astounding 31%. And worldwide, the music industry has shrunk from a $40 billion industry in 1999 down to a $26 billion industry in 2002. Hit records have been impacted 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. According to a November 2002 survey by Peter D. Hart Research, by a 2-to-1 margin, most consumers who say they are illegally downloading more music report that they're purchasing less. The same survey found that the main reason consumers aren't buying more music is that they get a lot of what they want for free by illegally downloading or copying it from others. 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 the same music for free over the Internet" - an

increase of 61% in just one year. These findings are consistent with the skyrocketing number of users of peer-to-peer ("P2P") file sharing software.

As of July 2002, KaZaa -- the most popular peer-to-peer ("P2P") file-sharing 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. All told, millions of users download over 2.6 billion copyrighted files (mostly sound recordings) each month via various peer-to-peer networks.

Of course, these networks are not limited to stolen copyrighted works. A GAO Report released earlier this year reveals that a significant percentage of the files available to these 13 million new users per month are pornography, including child pornography. And the problems are not just limited to the type of files available on these systems. Recent hearings in the House Government Reform and Oversight Committee and the Senate Judiciary Committee have also highlighted the serious privacy and security threats posed by P2P software, including the fact that many users on these systems are exposing their personal documents (e.g., tax returns, resumes, and medical records) to millions of other users.

Although there is no easy solution to these problems, one thing is clear: Verizon is reaping enormous financial benefits from the explosion in the use of P2P. It is particularly troubling to our industry that Verizon actively encourages its new subscribers to visit unauthorized P2P services -- instead of legitimate, licensed sites -- as their preferred source for music online.

Even as we speak, when new customers sign-up for Verizon DSL they receive a brochure entitled "Your Guide to Broadband Living & Content". Amazingly, on page 12 of the brochure, in the section that discusses music, Verizon tells its new subscribers, and I quote:

o "Once you're ready to groove to some tunes . . . [k]eep a couple of things in mind. Subscription sites do offer up MP3s to download; however, they typically don't offer music that is selling exceedingly well in stores. By contrast, the free sites are likely to have pretty much everything, but you may get pelted with some unwanted ads."

And people wonder why the copyright community is skeptical of Verizon's claim that the real issue is privacy and not their tacit acceptance and promotion of piracy by their subscribers.

The DMCA Balance:

So what do these statistics and Verizon's brochure have to do with the issues being addressed by the Committee today?

First, they help explain why RIAA's members with the support of a broad array of other organizations in the music industry representing artists, songwriters, music publishers, and record stores, took the action we announced yesterday.

Second, and perhaps more important for this hearing, they illustrate that Congress - following the leadership of this Committee -- saw the future in 1998 when it passed the Digital Millennium Copyright Act. The rampant piracy of music on the Internet is a true to life example of exactly the kind of problem Congress envisioned copyright owners would face in the digital world. Although P2P technology did not exist in 1998, Congress understood that the Internet and advances in technology would lead to an explosion in online theft of intellectual property.

Fortunately, at the time, Congress also had the wisdom and saw fit to include in the DMCA a fair and balanced procedure that enables copyright owners meaningfully to enforce their rights in the digital world. The framework established in §512 - commonly referred to as the DMCA information subpoena provision -- ensures that copyright owners, with the help of Internet Service Providers ("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. If you look around, this hearing room is filled with many people - people at the dias, people behind the dias, people at this table, and people in the audience - who spent countless hours discussing and negotiating what became §512. The final product of their efforts represented Congress's recognition 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.

Congress also understood that in a digital world, ISPs often would be the sole source for identifying individuals who are engaged in online piracy regardless of the type of technology they were using. So, in exchange for creating a framework by which copyright owners, with the assistance of ISPs, could expeditiously identify individuals engaging in infringing activities online, Congress exempted ISPs from any liability for the infringing activities occurring on or over the their networks and connections - subject, of course, to certain prerequisites. 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.

Keep in mind that absent the broad liability limitations of the DMCA, ISPs could face enormous monetary liability for the actions of their subscribers. With the current levels of piracy that liability could translate, at a minimum, to hundreds of billions of dollars. That fact helps explain why Judge Bates -- the federal district judge who presided over the enforcement proceedings between RIAA and Verizon -- concluded that: "[i]t 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]."

Verizon's Privacy Arguments:

Beyond the purely legal, statutory construction questions that have arisen concerning §512, Verizon and other ISPs now contend that there are privacy problems associated with the DMCA information subpoena. Before I address these concerns, it's important to make one thing crystal clear: no one has a privacy right to engage in copyright infringement on the Internet. Despite many novel arguments to the contrary, illegally sharing or downloading copyrighted music online is not a form of free speech or civil disobedience protected by the First Amendment.

It is also worth noting that during the first-round of litigation in our case, Verizon failed in any way to even mention or raise what they now contend is the biggest issue presented by this case: privacy. Rather than make their arguments in Court, Verizon chose instead to make their case in the court of public opinion.

Only after Verizon lost decisively on its legal arguments in the first-round of litigation did it decide that its privacy-related arguments warranted the Court's attention. The outcome, however, was no different. The district court found Verizon's privacy arguments as uncompelling as its legal arguments. Here is some of what Judge Bates specifically had to say about Verizon's privacy arguments:

? Verizon's customers should have little expectation of privacy (or anonymity) in infringing copyrights. Subscribers to Verizon's Internet services are put on clear notice that they cannot use Verizon's service or network to infringe copyrights.

? [A]s part of its corporate policy, Verizon alerts its subscribers at the outset that it will "disclose" individual customer information to an outside entity...when Verizon is served with valid legal process for customer information.

? [I]f an individual subscriber opens his computer to permit others, through peer-to-peer file-sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world.

? The [§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.

Although we agree with Judge Bates' reasoning and conclusions, I want to address some of Verizon's privacy arguments in greater detail.

As I understand Verizon's argument, disclosing its subscribers' identifying information (name, address, phone number, and e-mail) pursuant to a valid DMCA information subpoena threatens to violate its subscribers' privacy because the information subpoena process -- in their estimation -- is susceptible to abuse and does not provide the same protections afforded by a more traditional "John Doe" lawsuit. But Congress considered and decided this question back in 1998.

Ironically, the very principle ISPs profess to defend - the privacy of their subscribers - is at greater risk in a John Doe action than through the information subpoena provisions of the DMCA. There are statutory limits on the type of information a copyright owner can obtain via an information subpoena and the purpose for which that information can be used. Under a DMCA information subpoena, a copyright owner can only receive information that is necessary to identify and contact the alleged infringer - a name, address, phone number, and e-mail. More importantly, the copyright owner is statutorily limited to using that information exclusively for purposes of enforcing their copyright. Compare that to the John Doe alternative where a copyright owner can request anything relating to the ISP's subscriber account, including user habits, website visits, and payment records. Moreover, once that information has been provided to a copyright owner, there are no statutory restrictions whatsoever on how it can be used or to whom it can be shared. This fact makes Verizon's argument all the more suspect.

The information subpoena provisions of the DMCA illustrate that Congress not only understood the importance of protecting the privacy of end users, but also built in specific procedural safeguards designed to protect individuals from unwarranted disclosures of their information. As Judge Bates noted in his decision, the DMCA information subpoena "provides greater threshold protection against issuance of an unsupported subpoena than is available in the context of a [traditional] John Doe action."

The DMCA Information Subpoena Requirements & Safeguards:

As I stated previously, P2P software applications like KaZaA and Grokster 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. By logging onto these open networks and searching for files like any other user, the RIAA is able to identify the Internet Protocol addresses ("IP addresses") of individuals who are illegally uploading or downloading our works. Once we have obtained an IP address and matched that address to an ISP, the information subpoena provision of the DMCA allows us to enlist the help of the ISP in identifying those who steal our works.

Before obtaining any subscriber's information under the subpoena provisions of the DMCA, a copyright owner must provide to the clerk of a Federal district court:
o A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
o 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.
o Identification of the 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.
o A statement that the complaining party 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.
o A statement that the information in the notification is accurate, and under penalty of perjury, that the

complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
o 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.

A failure to adhere to any of these requirements is a justification for denying the subpoena and any copyright owner who misrepresents itself in satisfying these requirements is liable for damages, including attorney's fees. With these requirements and safeguards in mind, I want to address some of Verizon's specific arguments.

Anyone who has followed our ongoing litigation has heard Verizon boldly and repeatedly assert - without providing any examples or substantiation - that the DMCA information subpoena process is ripe for abuse at the hands of criminals. It is nothing short of amazing that in an effort to protect its bottom-line, Verizon would repeatedly make such baseless and desperate arguments. The RIAA, the copyright community as a whole and, more importantly, the Members of Congress who crafted the DMCA, would never defend or embrace a procedure that makes it easy for criminals to find victims. Verizon knows this and the public policy debate deserves better.

When I think of this argument, it reminds me of an old law school adage: when the law is not on your side, argue the facts; when the facts are not on your side, argue the law; and when neither the facts or the law are on your side, pound the table. In this case, Verizon risks breaking the table with its argument.

As Judge Bates noted in his second subpoena decision:

o "[I]t is noteworthy that although it has been nearly five years since § 512 came into effect, there is nothing in the record to indicate that the DMCA subpoena authority has been used for stalking or other fraudulent purposes."
o "Verizon's bald speculation of mistakes, abuse or harassment that has yet to occur to any degree (let alone to any substantial degree) since the statute was enacted is simply not enough,...[and] requirements in the DMCA should prevent such speculation from ever becoming a reality."

On a more practical level, however, Verizon's arguments simply don't hold water. Few, if any, criminals are willing to pay money and appear in Federal Court to identify themselves and leave a trail of information for authorities to follow. And even assuming a pedophile were willing go through the hassle of obtaining an anonymous IP address, forge a series of documents establishing his status as a copyright owner, and risk his own anonymity by appearing in Court, he can only obtain the adult ISP subscriber's contact information - and not any information relating to a child.

A cyber-pedophile looking for victims online is much more likely to get what he wants by simply sending an instant message to the unwitting young person who downloads an Olsen twins or pokemon file from the pedophile's share folder on KaZaa. And for the domestic abuser who already knows the identity of his victim, it's even harder to imagine that with all of the different ways to track someone down that he'd subject himself to the hassles and risks of the DMCA information subpoena process.

The facts and common-sense make clear that the cyber-pedophile and domestic abuser scenarios put forward by Verizon are little more than legal and public policy strawmen.

John Doe Lawsuits as an Alternative to Information Subpoenas:

Another argument put forward by Verizon is that requiring copyright owners to file a John Doe action in Federal Court will in some way provide greater privacy protections to its subscribers. In fact as discussed earlier, 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 infringers' information - exactly what Congress intended to provide copyright owners through §512. .

Not surprisingly, for ISPs, the John Doe approach is a win-win: they retain their broad liability limitation, while making it more difficult for copyright owners to obtain information - despite the fact that online piracy is skyrocketing. In stark contrast, for copyright owners, the John Doe procedure is a lose-lose: they no longer have access to an expeditious procedure for identifying alleged infringers and they are faced with significantly greater administrative and monetary burdens associated with enforcing their rights under the law. It's not hard to see why ISPs think this approach is better.

ISP Notice to Subscribers:
The RIAA and the copyright community as a whole understand the interest of the Committee and Congress as a whole in protecting the privacy of individuals. In the context of the DMCA information subpoena process, we also believe that protecting individual privacy reasonably and effectively already can be achieved through ISPs providing notice to their subscribers as soon as information is turned over to a copyright owner pursuant to a valid DMCA subpoena. In fact, nothing prevents ISPs from institutionalizing the practice of notice. The benefits of such a policy are clear --
o the subscriber is made aware that their information (name, address, phone number, and e-mail) has been turned over at the same time it's being given to a copyright owner pursuant to a valid information subpoena;
o the subscriber knows both who the information is being turned over to -- further helping to prevent any potential abuses of the process - and is made aware of the allegations warranting the disclosure;
o the subscriber is given an opportunity, in a timely manner and before any formal action is taken, to contact the copyright owner if the subscriber believes that the allegations underlying the subpoena are mistaken;
o the subscriber who is engaging in activity (other than piracy) protected by the First Amendment has an opportunity to contest the actions of the entity receiving the information.
The benefits of notice go a long way toward resolving any - perceived or real - privacy problems associated with copyright owners using the DMCA information subpoena. And when combined with the statutory use restrictions placed on copyright owners who obtain information under the subpoena provisions, we believe it is clear that no change in the law is needed.
Conclusion:
The copyright community believes that the DMCA information subpoena represents a fair and balanced process that includes important and meaningful safeguards to protect the privacy of individuals.
Thank you for the opportunity to testify today and I look forward to answering the Committee member's questions.