PIRACY OF INTELLECTUAL PROPERTY ON PEER-TO-PEER NETWORKS

HEARING

BEFORE THE

SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

SEPTEMBER 26, 2002

Serial No. 103

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

81–896 PDF WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., WISCONSIN, *Chairman*

HENRY J. HYDE, Illinois
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
BOB BARR, Georgia
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
LINDSEY O. GRAHAM, South Carolina
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL E. ISSA, California
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia

JOHN CONYERS, JR., Michigan
BARNEY FRANK, Massachusetts
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY

HOWARD COBLE, North Carolina, *Chairman*

HENRY J. HYDE, Illinois
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia, *Vice Chair*
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
LINDSEY O. GRAHAM, South Carolina
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
RIC KELLER, Florida
DARRELL E. ISSA, California
MELISSA A. HART, Pennsylvania

HOWARD L. BERMAN, California
JOHN CONYERS, JR., Michigan
RICK BOUCHER, Virginia
ZOE LOFGREN, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York

BLAINE MERRITT, *Chief Counsel*
DEBRA ROSE, *Counsel*
MELISSA L. MCDONALD, *Full Committee Counsel*
ALEC FRENCH, *Minority Counsel*

CONTENTS

SEPTEMBER 26, 2002

OPENING STATEMENT

WITNESSES

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

APPENDIX

PIRACY OF INTELLECTUAL PROPERTY ON PEER-TO-PEER NETWORKS

THURSDAY, SEPTEMBER 26, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, THE INTERNET,
AND INTELLECTUAL PROPERTY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 9 a.m., in Room 2141, Rayburn House Office Building, Hon. Howard Coble [Chairman of the Subcommittee] presiding.

Mr. COBLE. Good morning, ladies and gentlemen. The Subcommittee will come to order.

With the Subcommittee's permission, and the audience's indulgence, I'm going to deliver a longer than usual opening statement.

Prior to addressing the subject matter of today's hearing, I feel obliged to acknowledge that this is very likely the final time that I will preside over a hearing or markup as Chairman of the Subcommittee on Courts, the Internet, and Intellectual Property. While I won't close the door on examining other issues during the much-rumored lame-duck session, I can't say with certainty that we will meet again formally as a Subcommittee to conduct business in the 107th Congress. We will play that by ear.

If this is in fact my swansong, I want to say thank you.

I've been a willing participant in politics for a long time, but I confess that during my service as an elected official through these many years, I have never enjoyed policymaking more than I have with our Subcommittee. I was fortunate to have been surrounded by many decent, creative, and industrious people, Republican and Democratic Members, staffers, and those from other public and private quarters, who wanted to participate in the policy debates of the past 6 years. I'm reluctant to begin reciting names, because once you start on that course, you inevitably omit people who ought to be recognized.

But what has impressed me about everyone connected to our Subcommittee during my tenure as Chairman has been a collective willingness, for the most part, to work together, whatever our differences. I'm old enough to understand the rough and tumble nature of the legislative process, and to a very real extent, that feature is a healthy component of policymaking, reflecting as it does our constitutional right as Americans to express ourselves freely.

I believe, in this room, pardon my immodesty, but in this room, on this podium, and with many of you in the audience, I think we've done a better than average job for the past 6 years at ex-

pressing ourselves civilly, not just freely. And I think we may attribute that tone to the decency of those assembled herein.

Again, I thank you all very much for the generosity you've extended to me. I consider our accomplishments of the past 6 years to be better than average work. And I think during that time, folks, I think we have supported owners of copyrights, patents, and trademarks, both those who are financially struggling and those who are financially solvent, and the people who represent them.

Now, I am going to mention a couple names now. Howard Berman, who sits to my left—in fact, he is to my left generally, but now literally to my left. [Laughter.]

Howard has been a tremendous Ranking Member for the past 4 years. Barney Frank, the Ranking Member the first 2 years I served as Chairman. Alec French and his able Democrat staffers. Blaine Merritt and his able Republican staffers. Mitch Glazier, who preceded Blaine in that role. Eunice Goldring, who does the administrative work and keeps things away from the reefs and the rocks and the shoals on a day-to-day basis. And of course, Chairman Hyde, Chairman Sensenbrenner, and Ranking Member Conyers. And all Members of the Subcommittee.

In the event that we do have another hearing, Howard, I promise you won't have to hear this speech again. This will be the final speech.

Normally, as you all know, I deliver my opening statement, and then I recognize the distinguished gentleman from California. Today I'm going to reverse that procedure because the bill before us is Howard's bill. So I am going to now recognize the distinguished gentleman from California, the Ranking Member, for his opening statement. I will then give my opening statement. And then we'll recognize others who want to give opening statements.

Mr. Berman?

Mr. BERMAN. Well, thank you very much, Mr. Chairman. And I also may take a little more time than is generally allotted for my opening statement. The only thing I can assure you is that if I said everything I wanted to say, it would be a lot longer.

But I think, first of all, before getting to the legislation before us, I just wanted to take a moment to reflect on your tenure as Chairman. As you mentioned, it is very possible that your chairmanship of this Subcommittee ends—well, as Republican rules now stand, your tenure as Chairman ends with the end of the 107th Congress. And I really want you to know that I have deeply enjoyed and deeply value our relationship as Chairman and Ranking Member these past 4 years. I say this not in any pro forma way but sincerely, that you have led this Subcommittee through innumerable legislative and political challenges, and you have done so with characteristic charm, will power, and an always easygoing demeanor.

And your record I think is worth talking about for a moment because the accomplishments of this Subcommittee under your tenure have been really enormous. Think about it for a second. The Digital Millennium Copyright Act. The American Inventors Protection Act. We tried a long time with that legislation before you put it through this Committee, this House, and this Congress. The Sonny Bono Copyright Term Extension Act. The No Electronic Theft Act. The

Satellite Home Viewer Improvement Act. The Anti-Cybersquatting Consumer Protection Act. I even remember the Work Made for Hire and Copyright Correction Act. [Laughter.]

Mr. COBLE. If the gentleman will suspend, so do I. [Laughter.]

Mr. BERMAN. And the Madrid Protocol Implementation Act. And that we did a number of times, if I remember. And it looks like today may be the day that we finally send that to the White House. Other innumerable but less heralded bills.

I think that the American public owes you a debt of thanks for your dedicated service in your role as Chairman of this Subcommittee the past 6 years. I owe you a personal debt of thanks for including me as a partner in the leadership of the Subcommittee. I couldn't have been blessed with a better person to work with from the oppose side of the aisle than you, and I'm very grateful for having had the opportunity to work with you and to serve with you.

Now, to turn to the oversight hearing on the P2P piracy issue and the legislation.

I think there have been some truly outrageous attacks on the P2P Piracy Prevention Act, and I want to take this opportunity to try and set the record straight. When we first introduced the P2P piracy bill, the Chairman and I, as well as Mr. Smith and Mr. Wexler, I never expected that anyone would challenge the underlying premise of the bill, namely that copyright owners should be able to use reasonable, limited, self-help measures to thwart rampant P2P piracy. But there are, it turns out, folks who actually challenge that premise.

The head of a big trade association claims it's legal to make unauthorized distributions of copyright works to 100 million P2P users. P2P software companies claim that, even if illegal, P2P piracy causes no harm. Representatives of the computer industry say that only record companies suffer harm, and they deserve it for charging too much. Others vaguely theorize that copyright owners' self-help will threaten security or privacy. And still other piracy profiteers attempt to thwart any solution to P2P piracy and then throw their hands up and say it's an insoluble problem.

Let's start with a basic fact: Unauthorized distribution or downloading of copyrighted works on public P2P networks is illegal. To paraphrase the 9th Circuit in the Napster case, public P2P users "who upload file names to the search index for others to copy violate a copyright holders' distribution rights. P2P users who download files containing copyrighted music violate a copyright holder's reproduction rights." Any attempt to say otherwise is a bald-faced attempt to rewrite very well-settled law.

Let's move to another indisputable fact: Massive theft of copyrighted works is the predominant use for public P2P networks today. There are now approximately 3 billion—3 billion—files P2P downloads a month—a month. The vast majority of these downloads contain copies of copyrighted works for which the copyright owners receive no compensation.

Now, another fact: P2P piracy doesn't just affect the bogeymen—record companies and movie studios. P2P piracy destroys the livelihood of everyday people.

What do piracy profiteers have to say to Linn Skinner, a Los Angeles needlework designer whose livelihood has been destroyed by Internet piracy? Or about Steve Boone, a Charlotte small-business man—notice, Los Angeles, Charlotte—who has watched P2P piracy decimate his karaoke tape company? How do they respond to Mike Wood, a struggling Canadian recording artist who believes P2P piracy will derail his recording career before it gets off the ground? What do piracy profiteers say to the vast majority of songwriters who make less than $20,000 a year and have yet to make one thin dime from the massive P2P piracy of their works?

Songwriters can actually quantify their P2P piracy losses. By statute, a songwriter is both entitled and limited to collecting 8 cents for every digital phonorecord delivery of sound recordings containing her songs. Each illegal P2P download of a song robs the songwriter of that 8 cents.

Those 8 cents may not seem like much, but multiply 8 cents by the reported 3 billion monthly P2P downloads. It calculates out to $240 million a month. Even one-tenth of that amount represents real money to the 5,000 American songwriters.

Now another fact: If piracy profiteers were truly concerned about security and privacy threats to P2P users, they would address the security and privacy threats posed by the P2P networks themselves. A recent white paper by the University of Tulsa Center for Information Security details how KaZaA, Gnutella, and other popular P2P networks expose P2P users to spyware, Trojan horses, system exploits, denial of service attacks, worms, and viruses. A joint paper by Hewlett-Packard labs and the University of Minnesota details how the vast majority of P2P users are exposing personal information, such as credit card numbers, to every other P2P user. In fact, the United States courts, the House, and the Senate all block the use of public P2P networks because of the security concerns they pose.

Do the piracy profiteers talk about these real security and privacy concerns? No. And you know why—because it is the piracy profiteers who point the spyware on the computers of P2P users so they can surreptitiously collect their personal information and sell it to third parties.

Another fact: P2P companies could design their software to stop piracy, but they don't. Grokster has designed its P2P software to filter out pornography, but has it ever tried to filter out copyright infringements? Napster claimed it couldn't stop piracy, but after the court ordered it to do so, it suddenly found a way to stop most if not all piracy on its networks.

Rather than looking for solutions to piracy, P2P companies are designing their systems to be better piracy tools. Both Morpheus and KaZaA have upgraded their software specifically to impair the ability of copyright owners to proliferate decoy files through the networks.

Based on all these facts, what can an objective person conclude other than many companies plan to profit from piracy and have no intent or desire to stop it?

I look at these facts and figures, at the faces of copyright owners, and I see a problem in desperate need of a solution. P2P piracy must be cleaned up and cleaned up now. The question is, how?

I think my P2P piracy bill is an important part of the solution. The Peer-to-Peer Piracy Prevention Act is quite simple in concept. It says that copyright owners should not be liable for thwarting the piracy of their works on P2P networks if and only if they can do so without causing harm.

You might reasonably wonder why we need to pass legislation giving property owners the right to protect their property against theft. After all, the U.S. Supreme Court has held that "an owner of property who seeks to take it from one who is unlawfully in possession has long been recognized to have greater leeway than he would have but for his right to possession." The claim of ownership will even justify a trespass and warrant steps otherwise unlawful.

The problem is that a variety of State and Federal statutes may create liability for copyright owners engaging in otherwise justifiable self-help. That's not fair. Copyright owners should have the same right as other property owners to stop the brazen theft of their property. The P2P piracy bill simply ensures that the law will no longer discriminate against copyright owners.

Obviously, it is critical that a liability safe harbor be appropriately limited. In drafting the P2P piracy bill, I tried to ensure that only reasonable self-help technologies would be immunized and the public would be protected from harm and that overreaching or abuses by copyright owners would be severely punished.

The most important limitation in the bill is the narrow breadth of the safe harbor itself. The bill says that copyright owners get immunity from liability under any theory but only for impairing the unauthorized distribution, display, performance, or reproduction of their own works on public P2P networks.

If the copyright owner's impairing activity has some other effect, like knocking a corporate network offline, the copyright owner remains liable under whatever previous theory was available.

Some claim that the bill is not limited that way. Their claim appears to be that the bill gives a copyright owner immunity for anything she does as long as it has the effect of stopping piracy on a P2P network. By their logic, the bill allows a copyright owner to burn down a P2P pirate's house if the arson stops the pirate's illegal file trading. Clearly, the bill says nothing of the sort, and no judge or disinterested party could read it that way.

The bill specifically states that a copyright owner cannot delete or alter any file or data on the computer of a file trader. Thus, a copyright owner can't send a virus to a P2P pirate. It can't remove any files from the pirate's computer. And it can't even remove files that include the pirated works. The safe harbor does not protect a copyright owner whose anti-piracy actions impair the availability of other files or data within the P2P network, except in certain necessary circumstances.

Some folks have raised concerns about this provision, and we're thinking about alternative language that could resolve their concerns. The bill denies protection to a copyright owner if her anti-piracy action causes any economic loss to any person other than the P2P pirate. The safe harbor is also lost if the anti-piracy action causes more than de minimis loss to the property of the P2P pirate.

Finally, the safe harbor is lost if the copyright owner fails to notify the Attorney General of the anti-piracy technologies that he or she plans to use or fails to identify herself to an inquiring file trader.

Obviously, these limitations would be meaningless if copyright owners did not have adequate incentive to obey them. The P2P piracy bill provides such incentives by subjecting transgressing copyright owners to more liability than they have under current law.

This is a critical point. If a copyright owner falls outside the safe harbor, an aggrieved party could sue the copyright owner for any remedy available under current law and for an additional civil remedy created by the P2P piracy bill. The bill also gives the U.S. Attorney General new power to seek an injunction against transgressing copyright owners.

The potential for liability under this wide variety of remedies provides copyright owners with strong incentives to operate within the strict limits of the safe harbor.

I think the P2P piracy bill provides a strong starting point for legislation enabling copyright owners to use reasonable self-help to thwart P2P piracy. I don't claim to have drafted a perfect bill. I welcome suggestions for improvements. I know, however, that while I will listen carefully to those who wish to solve the P2P piracy problem, I'm not that interested in being solicitous of those who wish to profit from it.

Thank you very much, Mr. Chairman, for your indulgence here.

Mr. COBLE. Thank you, Mr. Berman. And I thank you as well, Howard, for your generous comments at the outset.

We normally restrict opening statements to the Ranking Member and the Chairman, but because of the widespread interest that's been focused upon this issue, I want to ask my Members, how many would like to make opening statements?

Mr. ISSA. I'll submit mine for the record, Mr. Chairman.

Mr. COBLE. If you would.

And I think it's in order that Mr. Berman exceeded the 5 minutes, because this is his bill, and I think that was in order. But I would ask the rest of you, if you would, to confine your opening statements, if you can, to within the 5-minute framework, because we do have a busy day on the floor today.

I have been the beneficiary of complaints regarding bills that I have introduced, but I have never received such notoriety from a bill that I did not introduce. I co-sponsored this bill. And if Howard Berman asked me today to co-sponsor it, I would do so again.

As Chairman of this Subcommittee—and, for that matter, as Members of this Subcommittee—I think it is our responsibility to promote efforts to reduce infringement or piracy of intellectual property. To that end, this hearing is intended to explore the problem of piracy on P2P networks and possible remedies.

As Mr. Berman just said, if you have suggestions, come forward with them. We're seeking solutions.

Many people have inserted scare tactics into this. If you can successfully play with a scare tactic and frighten people, you have a leg up. I've read in different articles where anyone who supports this legislation is in the pocket of Hollywood, and I take umbrage with that for two reasons. A, it implies that only Hollywood bene-

fits from anti-piracy approaches. And B, it implies that we're in somebody's pocket, and I don't think there's anyone on this Subcommittee that's in the pocket of anyone.

Recent technological advances have created a digital environment that is almost solely devoted to the unauthorized use of copyrighted works. In other words, P2P network customers are primarily using the program to obtain music, movies, software, photographs and other works without paying for the product.

Let me be clear at the outset that I am not opposed to P2P networks. In fact, I believe that P2P networks have potentially beneficial uses that will play an increasingly important role in how business is conducted.

I am, however, opposed to the rampant stealing that is occurring on these networks. While not every download is an infringement, statistics clearly reveal that a vast majority of them are in fact illegal. Between 12 and 18 million movie files and 2.6 billion music files are downloaded for free on the P2P networks each month. And the U.S. Customs Service reports that certain elements within the online community are responsible for at least $1 billion annually in lost sales of computer games, business software, music, and movies.

This translates into huge economic losses for not just large media companies but also individual songwriters, photographers, graphic artists, and software developers all over the country.

The question, then, is, how do we stop the massive piracy on P2P networks? Today we will hear from the panel about potential answers to the P2P piracy problem and their implications.

The gentleman from California, Mr. Berman, has developed one solution, which he believes will work. It is my understanding that this bill is intended to clarify that copyright owners may utilize new technologies to protect their property as it is distributed on P2P networks. No doubt the panel will also comment on the merits of the proposed legislation.

I'm also reminded of ongoing private negotiations between the content industry and the technology providers to find a technological solution to digital piracy. It is furthermore my understanding that the process nearly reached a consensus on a watermark technology for use on DVDs that could also have important implications for preventing P2P piracy.

I strongly support efforts by industry to resolve these issues through private agreements. I encourage both sides to redouble their efforts and to narrow their differences. And should this process fail to reach an agreement, it is very likely, I think, that this Subcommittee may well examine the reasons for its failure at a later date.

I anticipate that this hearing will provide lively debate on a complex and controversial issue. I look forward to learning more about the status of P2P piracy problems and potential solutions to the problem of digital theft.

I am now pleased to recognize the gentleman from Virginia, Mr. Boucher, for 5 minutes.

Mr. BOUCHER. Thank you very much, Mr. Chairman. Let me say at the outset that I appreciate the Subcommittee holding a hearing on the matter of music distribution across the Internet. But I'll

have to confess a preference for a somewhat different focus than that of this particular hearing.

There is a need, I think, for legislative action in this Committee to facilitate the lawful distribution of music across the Internet in a manner that assures that all owners of copyrights are paid. Mr. Cannon and I have introduced a comprehensive measure, the Music Online Competition Act, which, if enacted into law, would help achieve that goal.

The Copyright Office has also recommended legislation that would help achieve that goal. The recording industry can achieve that goal if it will simply place entire inventories on the Web for permanent, portable downloading at a reasonable price per track.

There's a recent Jupiter Media Metrix study that shows that two-thirds of the public values the availability of a broad inventory of music, the assured quality of the download, and the ability to keep the music permanently and move it from one player to another in the personal environment as more important considerations than price. These two-thirds of the public would clearly be willing to pay a reasonable price if the other elements of quality, availability, and portability are present.

In my view, the recording industry does not need the legislation which the Subcommittee is considering today. It should put entire inventories on the Web for permanent portable download at a reasonable price. That's the way to compete with the lower quality free peer-to-peer file-sharing services.

Turning to the bill at hand, I question at the outset what it is that the industry wants to do that would be authorized under the provisions of this bill that it can't do under current law. Spoofing is allowed now. Decoys are allowed now. Redirection to legitimate Web sites is allowed now. I hope that the witnesses will be very specific about what it is that the industry wants to do by way of self-help that it can't do at present.

And I have some other questions. Would any of these intended self-help mechanisms harm innocent Internet users by perhaps slowing down the speed of a shared network, such as a cable modem service? Would any of these mechanisms permit the recording industry to intrude into the personal computer space of an Internet user? And if so, what are the implications of such intrusions for the privacy rights of individuals? If any damage is done to the hardware, software, or data owned by an Internet user, how would the damaged party know who to proceed against? After all, no notice to him is required under the bill that his space is being invaded or who is doing the invading. And so if he's damaged, how does he know who to recover from?

What assurance will there be that material which is protected under the fair use doctrine will not be blocked or removed by a self-help invasion? What are the implications for the Internet's functionality when the inevitable arms race develops and countermeasures are used to block self-help mechanisms? I can imagine that if the recording industry launches what amounts to a denial of service attack against Internet users, that denial of service attacks will, in turn, be launched against the industry, with broad, adverse effects on Internet speed to the disadvantage of Internet users generally.

These are a few of the matters that concern me. And I very much hope that these questions will be addressed by the witnesses this morning.

On a personal note, Mr. Chairman, let me extend to you also my thanks for the way in which you have conducted the business of this Subcommittee. You and I on occasion have disagreed on substance, but we've always disagreed agreeably. And I want to commend you, Mr. Chairman, for the fair and evenhanded way in which you have conducted the business of this Subcommittee. It's a pleasure serving with you in the Congress. I look forward to many future years of our service together, and I wish you well.

Thank you.

Mr. COBLE. Thank you, Mr. Boucher. I appreciate that.

The gentleman from Virginia.

Mr. GOODLATTE. Mr. Chairman, thank you.

Mr. COBLE. If the gentleman would suspend, I appreciate, Rick, your meeting the 5-minute rule. If you all could work with 5 minutes, because we are going to be called to go to the floor ultimately.

I recognize the gentleman from the valley.

Mr. GOODLATTE. Mr. Chairman, I thank you also for holding this hearing on a very, very important issue which goes to the heart of the use of the Internet by the public and the need to protect valuable copyrighted works by the creators and owners of those works.

I have not yet co-sponsored this legislation. I am very, very concerned about piracy of copyrighted works. And I am very, very supportive of efforts to try to combat that. I am, as many of you may know, the author of the NET Act, which passed the Congress several years ago, was signed into law, that gives new tools to law enforcement to go after those who steal copyrighted works or give away for free the copyrighted works that do not belong to them.

However, I am also concerned about what this legislation's implications are for the use of the Internet. Will it work, or will it simply cause an escalating war of various technologies that will not lead to the best utilization of the Internet?

I note the chart over there that indicates that those who promote these networks have already developed tools that will bypass some of the technology that those who would protect copyright want to deploy. They've already found ways to detect video files that are so-called spoof files or bogus files.

And so I want to know the implication of that. I hope these witnesses today will share with us their concern about that.

And I am very, very concerned about the misuse of P2P networks. I happen to think that they provide a very good service and a very good function for people to get access to a multitude of information that's in the public domain. However, for things that are not in the public domain, for things that are privately owned, like copyrighted works, they have, in my opinion, a responsibility to come forward and to deploy the technology that apparently would bypass and detect the spoof files obviously would also detect legitimate copyrighted files, and it should be deployed in a such a way to protect those files. And I'd like to know why that is indeed not being done to protect copyrighted works and why instead the largest peer-to-peer network, KaZaA, has fled the United States, via the Netherlands to Australia, and now finds itself on the island of

Vanuatu as its principle location for doing business obviously for the purpose of evading the ability of those who would protect copyrighted works and enforce the laws of the United States and other nations to do so.

So, Mr. Chairman, I will listen with great interest in how this legislation will work and want to hear from these witnesses and their opinion on the legislation and will reserve my judgment.

Thank you very much.

Mr. COBLE. I thank you, sir.

I am pleased to recognize the gentlelady from California for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

I think there's growing consensus that advanced peer-to-peer applications are the next killer application that will drive growth in the computer hardware, software and equipment industries as businesses and consumers demand faster and more powerful PCs. The P2P applications also have the potential to give consumers a reason to embrace broadband.

But today we're not here to discuss ways to harness the potential and encourage investments in peer-to-peer applications. We're here solely to focus on ways to help copyright owner and holders sabotage peer-to-peer networks if they think their works are being infringed.

Now, illegal file-sharing is a problem. But the breadth of the current proposal is of concern to me. Among other things, it seems to give copyright holders the power to launch denial of service attacks and other invasive self-help measures. It appears to authorize and make it easy for copyright holders to delete an individual's files if they receive authorization in a non-negotiable licensing agreement. And it would make it nearly impossible for consumers to seek redress against copyright holders that cause unwarranted damage, much less find out who caused the damage.

One of the most disturbing parts of the current discussion to me is that the interests of consumers tend to be overlooked here in the halls of Congress. We have major industries, including technology and entertainment industries, but the consumers' interests sometimes don't get attended to. And while some would say there are millions of pirates—and there are people who are unfairly taking advantage of peer networks—we also know that millions of consumers want digital distribution. So we can debate the spoofing and the decoys and the interdiction, but the problem of online privacy will not be solved, in my judgment, until those who have content and those in the technology world give consumers what they want: digital distribution that is affordable, secure, and user-friendly.

The fact is that peer-to-peer networks, like the Internet, are here to stay. And I hope that this Committee will some day have the ability to explore ways to harness their potential so that users can get what they want and that content and copyright holders can be treated fairly.

I would also like to note, Mr. Chairman, how much I have enjoyed serving with you on this Subcommittee. We have not always agreed, but the disagreements have never been partisan. This has

been sort of an island of nonpartisanship in an oftentimes choppy sea of partisan nuttiness.

And I would also like to thank Mr. Berman, who I admire a great deal and consider a friend. And while I do not support this current effort, I know that his motives are nothing but honorable. And I have a great hope that we will be able to pursue these issues agreeably and successfully in the next Congress.

And I yield back the balance of my time.

Mr. COBLE. I thank the gentlelady. Thank you, Zoe, for your comments.

The gentleman from California.

Mr. ISSA. Thank you, Mr. Chairman. And I, too, would like to thank Mr. Berman for producing yet another bill that, although I do not co-sponsor it, in fact points up a problem that has not gone away, a problem that sooner or later has to be dealt with by this body.

I hope as we go through the hearing process and probably in the next Congress, that this bill or its successor becomes a bill that in fact we can all embrace.

I would like to say here today that I have the good fortune of knowing, I believe, the association executive who made those statements. And I would like to disassociate myself with anyone who believes for a minute that Napster was in fact not a very organized way of stealing intellectual property, just as KaZaA is an extremely good example of exactly what this body, this Administration, and both the copyright holders and the technology community must ban together, with laws or with association work, and prevent. And I would call on that association and others to redouble their efforts to find a solution that doesn't require a clumsy legal mandate.

Mr. Chairman, I'd like to put my official opening statement in the record.

Mr. COBLE. Without objection.

Mr. ISSA. I would like to just comment on two things in opening, so that hopefully we set a tone for this.

First of all, I got on this Committee not because I'm an attorney but because, in fact, I was probably the only person to come before this body who ever was ripped off for their intellectual property, went to court, won judgments, enforced the judgment, collected millions of dollars that were taken from my company by people who had no respect for a piece of paper and felt that their product outranked our piece of paper, our inventions.

So I come here with a particular bent that in fact statements that were made here—which I do not want to insult people who made them; I think they were made without perhaps regard for the words. Statements like "reasonable prices" are in fact not part of the copyright, patent, or trademark debate. A reasonable price may be the price you charge yourself if you're charging others. That's a fair and similar price.

But I want to make it very clear that I for one will not ask that online services be mandated to meet an artificially different price. I believe they should. That's a personal opinion. But I think it's important that the copyright holders understand that if they choose to put their product on at $29.95 or at $.99, that is a business deci-

sion that they have to make consistent with the constitutional protection that they were clearly granted by our Founding Fathers.

And I think as we go through the debate, hopefully we can eliminate this theory that piracy is the result of unreasonable prices by the copyright holders. I think that's often something that slips into the debate. And although certainly you can undercut the pirates to a certain extent, you can never get below someone who didn't pay for the product, and particularly on the Internet.

In closing, Mr. Chairman, I think that this legislation being talked about is the most important thing that we can do in this Congress. But in the next Congress, if we cannot orchestrate industry-led solutions, I have no doubt that this Committee must act and must find a piece of legislation that is as least flawed as possible. And I look forward to working with all parties on that.

Thank you, Mr. Chairman. I yield back.

[The prepared statement of Mr. Issa follows:]

PREPARED STATEMENT OF THE HONORABLE DARRELL E. ISSA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you Chairman Coble for holding this Oversight Hearing on "Piracy of Intellectual Property on Peer-to-Peer Networks (P2P)."

I thank the Ranking Member of this Subcommittee, Howard Berman from California, on introducing H.R. 5211, which is an attempt to address the issue of P2P networks and piracy. I hope that this legislation helps to shine some light on a very important issue.

As a former businessman who owns numerous patents and trademarks, I understand the need to protect intellectual property. When I encountered infringers of my trademarks or companies that stole my patents to market their products, I was forced to litigate. Unfortunately, the copyright owners, because of the presence of P2P networks and the proliferation of new online users downloading pirated material, have had to follow the same course as I and have not been as successful.

Since the introduction and immediate success of Napster, the Internet has been viewed by many as a means to download free music. Now, with the demise of Napster, new P2P networks, like Kazaa, Morpheus, BearShare, Grokster and Gnutella, provide channels for downloading music and movies with digital quality. The ease in which one can download pirated material is disheartening for me as an intellectual property owner.

Copyright owners have attempted to discourage the piracy taking place on P2P networks by different means including litigation and most recently, interdiction, redirection, decoys and spoofing. Still, P2P networks are successfully evading the law by fleeing to foreign countries or taking refuge on offshore locations. Unfortunately, with each illegal P2P network that is shut down a new one takes its place. Each new P2P network seems to be a more decentralized program that will be more elusive to litigate. In the not-too-distant future, we will see other programs that will provide pirated material on bigger, better, faster nodes. The status quo is not acceptable for the copyright owners, nor is it in the interest of the American People.

Without swift action, P2P networks that advocate pirating copyright material, without just compensation of any sort, will continue to be pervasive on the Internet. An industry-led solution is needed, but it will take coordination from the copyright owners, the consumer electronics industry and the software manufacturers in order to be successful. Collectively, they have the technology and ability to confront the infringement of copyrighted material on P2P networks. If a unified solution is not brought forward soon, or no consensus can be reached, I have no doubt Congress will be forced to pass legislation that is "least flawed" to address this problem.

As we begin this journey, I encourage this subcommittee to hear testimony from additional witnesses, including content holders, software manufacturers and the consumer electronics industry. Their involvement is very important if we are to curtail piracy. I want to work with Chairman Coble and the next chairman of this committee on H.R. 5211 and any other bill that provide the tools necessary for fighting piracy that we can all embrace. H.R. 5211 will help to focus the attention of the members of this subcommittee and an issue that is spiraling out of control.

I thank the Chairman for scheduling this hearing today and look forward to the testimony of this distinguished panel of witnesses.

Mr. COBLE. I thank the gentleman.

The Chair is pleased to recognize the distinguished gentleman from Massachusetts.

Mr. DELAHUNT. I don't have an opening statement, Mr. Chairman. But let me join the others that have appropriately sung your praises.

As my friend Zoe Lofgren indicated, I think her reference was an island of bipartisanship in a sea of controversy. Oh, how eloquent and poetic and true.

You have earned the respect, the admiration, and the friendship of all of us who have served on this Subcommittee.

Mr. COBLE. You all are making an old man feel mighty good this morning. Thank you, Bill.

And I notice most of my accolades are coming from the Democrat side, not the Republican side. [Laughter.]

Mr. DELAHUNT. That's why we call it an island of bipartisan. [Laughter.]

Mr. COBLE. I thank you, Mr. Delahunt, very much.

Mr. ISSA. Howard, we know you're not going anywhere. You're just ending your Chair. We kind of figure we'll still have you around to sing your praises.

Mr. COBLE. Oh, very well. [Laughter.]

The gentleman from Florida.

Mr. KELLER. Thank you, Mr. Chairman. I, too, join in appreciation of your good work as the Chairman.

I think there is unanimity in the concept that stealing is bad and there should be consequences. But as a practical matter, other than this self-help bill that Mr. Berman has drafted, I'd like to hear what the solutions are from the witnesses. And when I say the solution, just a practical solution, not legal mumbo-jumbo because this is the way I as a layman see it: Universal wants to put out the new Celine Dion CD, let's say. So they ship the CD off to radio stations 4 months in advance to promote their best single, what they perceive to be their best single. I think it was called "A New Day." And some college student, an 18-year-old kid, at one of these radio stations borrows that CD for the night and puts it upon the Internet, brings it back the next day. And so 4 months before this CD is released, it's available on the Internet for free.

The question is, what do we do here? What's the remedy?

Well, criminal enforcement has been mentioned in some of your statements. We can ask Ashcroft or our local prosecuting attorney to do something about it. And they'll probably that they're sure sensitive to this but they have murders and terrorists and Mafia kingpins and drug lords that they have to prosecute with their precious dollars. Civil enforcement has been mentioned as a second remedy. They could hire a Sullivan & Cromwell and spend $200,000 and get a judgment against this kid, and he certainly has no money to pay it. So that's money down the drain.

It would probably be a PR nightmare for Celine Dion to go after this little kid.

There's the use of licensed services that are legal. Well, that's a great concept, I think. But why would people pay $20 a month when they can get it for free over the Internet?

The fourth thing, maybe Congress should come up with some technological solution for the industry. There are a lot of smart guys around here, but I don't know how many Ph.D.s we have who spend their free time coming up with secretive, complicated encryption devices that are going to work.

I wish Lindsey were here, because he's fond of saying that he got 800 on his SATs and he's one of the smart ones here in Congress. [Laughter.]

So we're left with technological self-help measures. And that to me is about what you're left with. And if that's not the solution, then please tell me, as a practical matter, what is the solution, in your testimony, because I can't see any other solution.

So thank you for coming here today.

Mr. BERMAN. Would the gentleman yield?

Mr. KELLER. Yes, I'd be happy to.

Mr. BERMAN. I was just curious why you thought you could get that firm to get that judgment for $200,000.

Mr. KELLER. I know that's cheap, for any of the firms. I don't want to do promotion for them.

But please advise me on the practical solutions, because I'm certainly interested.

Mr. Chairman, I'll yield back.

Mr. COBLE. I appreciate that.

I'm told that we have a vote on, but I think I can recognize——

Mr. BERMAN. That's just the warning.

Mr. COBLE. I stand corrected.

The other gentleman from Florida, Mr. Wexler.

Mr. WEXLER. Thank you, Mr. Chairman. I would like to join in the chorus of people who have applauded the way in which you have conducted yourself as Chairman of this Subcommittee. Your evenhandedness and decency and fairness is all too uncommon in this process. And it has been a great honor to be a part of your Subcommittee.

With your permission, Mr. Chairman, I would like to use my time for a brief demonstration.

Mr. COBLE. Without objection, that will be done. And thank you for your comments, Mr. Wexler.

Mr. WEXLER. Thank you.

Before the issue of peer-to-peer piracy came up, I for one had never heard of peer-to-peer networks or MP3 files. And I thought it might be helpful to walk the Subcommittee through a demonstration of just how easy it is to download pirated music from these peer-to-peer networks. And the Members, if they wish, can follow on the screen.

Once someone downloads a peer-to-peer program like KaZaA, downloading pirated music is as easy as surfing the Internet. This search you are watching was taped two nights ago. The reason this demonstration had to be taped is that the House of Representatives has a firewall to prevent peer-to-peer network activity because these networks are too risky for security and piracy reasons to be considered safe for use on House computers.

So as you can see on the bottom right-hand corner of your screen there, this search is a recording from Tuesday night at 8:23 p.m. All you have to do to steal copyrighted material is click the search

button and type in the name of the song or movie you want to download.

Since we have a copyright owner testifying before this panel this morning, we searched for the song that Mr. Galdston wrote for Vanessa Williams, "Save the Best for Last." We just type in "Vanessa Williams," "Save the Best for Last." All of these hits come up. Each one of these lines is an MP3 file that has been uploaded to the peer-to-peer network without the permission of Mr. Galdston. And if Mr. Galdston will forgive us, we can just double-click any of these titles to download the song onto that computer right there.

While we wait for the song to finish, let me point out, as you can see on the bottom of the screen, when we recorded this demonstration, we weren't the only ones. Almost 3 million users were online stealing music, so-called sharing, almost 500 million individual files. This is just an ordinary Tuesday night in America on one of the many popular peer-to-peer networks. It is mind-boggling to realize that tens of millions of songs are being stolen every night in America.

In only a few seconds we were able to steal the property of Mr. Galdston. We have a copy of the song as an MP3 file at near-CD quality. We can burn it onto a CD with other downloaded songs or share it on other peer-to-peer networks ourselves.

Anyone can download music and movies. It's easy. Sharing music and movies on peer-to-peer networks appears to have no negative consequences. You can get the entertainment you want for free and it seem harmless enough. Not so.

Mr. Galdston and all the other songwriters and musicians who make their living writing and recording music get hurt. Without the income from their copyrighted property, many musicians will not be able to continue creating the music we love to listen to, and we will lose this important American business. We will lose this integral part of American culture as well.

And the impact is felt by more than just the copyright owners. Local music and movie stores are facing dramatic drops in sales. With the economy as it is, we cannot afford do allow peer-to-peer theft to cripple the American economy or to stunt the development of new music and movies.

As you can see on the chart next to the screen, 2.6 billion—billion—songs are downloaded every month. KaZaA brags on its own Web site—this is KaZaA—that over 120 million users have downloaded its software.

And the problem is not limited to songs. Between 12 and 18 million movies are downloaded from peer-to-peer networks each month as well.

One-half of all teenagers in America have downloaded music for free, with two-thirds of them saying they buy less music now that they can essentially steal it over the Internet so easily.

I am a sponsor of Mr. Berman's bill because given the severity and magnitude of the problem, we are left with no choice but to take action. Every one of these 2.6 billion downloads per month is a theft no different than going into a store and putting into you bag and walking out without paying.

We cannot realistically expect the criminal justice system to prosecute these cases. We need the Berman bill so that the copyright owners can protect their property themselves, just as individuals are allowed to protect their possessions from theft.

Thank you, Mr. Chairman, your indulgence.

Mr. COBLE. I thank the gentleman from Florida.

Mr. GOODLATTE. Will the gentleman yield?

Mr. COBLE. The gentleman's time has expired. We'll get to this in a minute.

The other gentleman from Massachusetts, Mr. Meehan.

Mr. MEEHAN. Thank you, Mr. Chairman. And I, too, want to join my colleagues in thanking and congratulating you for your outstanding service to this Committee. Today is really "Howard Coble Day" in the House of Representatives. And I thank you for your outstanding leadership.

I also want to thank the Chairman for calling this hearing, as well as Congressman Berman, for taking the lead on the issue of peer-to-peer piracy.

Peer-to-peer piracy is theft, period. The illegal downloads of free music, which we've just seen demonstrated, of music software, movies from an Internet site, is really no different than lifting a CD or a DVD off the shelves of a Best Buy. And when you have two identical products—one that is free that you can download, as millions and millions of Americans apparently are, and then you have another one that has a price tag—obviously, free wins every time.

And throughout all of the debate over this issue, I've yet to hear a single person dispute those simple facts. Instead of admitting those basic facts and trying to find a common solution, we have seen a whirlwind of charges hurled at the Chairman and Congressman Berman. In fact, I've rarely seen the amount of vitriol, unsubstantiated charges surrounding a piece of legislation as I've have with Congressman Berman's bill. And it kind of makes me wonder: Has anyone really read this bill?

If your goal is to preserve peer-to-peer piracy, then just come out and admit it. If at heart you simply don't believe in intellectual property, then just say so.

I agree that the content provider community has been too slow in finding ways to offer their products digitally. And I'm willing and eager to listen to amendments to this legislation. Certainly, no bill is perfect. But if you have a good-faith, reasonable alternatives, then I'm more than willing to hear them. But we have to take a first step, if we believe in American music and believe in American entertainment.

I mean no offense to countries with weak intellectual property laws, but I would much prefer to watch a movie from Hollywood than average fare from Taiwan.

This bill is a good first step toward stopping a very serious problem.

Thank you, Mr. Chairman.

Mr. COBLE. Thank you, Mr. Meehan. And thank you for your kind words as well.

The gentlelady from Wisconsin.

Ms. BALDWIN. Thank you, Mr. Chairman. I, too, would like to acknowledge the good humor and graciousness with which you have chaired this Committee and your very capable stewardship.

Times have certainly changed since I had my cassette tape recorder sitting beside my radio, and I sat beside both, ready to dash to the record button when my favorite song came on.

In acknowledging the challenges faced by the industries represented at the hearing today, I know that we are truly searching for constructive answers. I look forward to the testimony and joining the Committee Members in fashioning the appropriate solutions.

Mr. COBLE. I thank the gentlelady.

The gentleman from New York.

Mr. WEINER. Thank you, Mr. Chairman. I want to join in the accolades being paid to you. And I also find it unusual that no one has commented on your exotic, Southern, I guess it's Staten Island accent that you govern this Committee with. [Laughter.]

And I want to thank you for how well you have conducted these hearings.

At the same time that many of us have reached the conclusion that the best policy for Government to take in the explosion of the Internet was probably to take a few steps back and to allow some of the technological problems, some of the content problems that troubled folks, to be worked out by the marketplace, worked out by technological solutions, we've seen a certain level of schizophrenia about this problem. At the same time that music companies and producers are trying to figure out ways to stop this pirating of intellectual property, just about every day in the newspaper or on television you see hardware makers advertising that their products will make it easier for you to break the law.

When you have an iPod advertised that you can have 3,000 songs, rip it, zip it, and go, or something like that, you know, it is clear that, on one hand, technology is working to make it easier to commit these crimes, to make it easier to commit piracy. When you have that dopey guy from Dell telling you how great the system is. It lets you go to campuses and how it can download faster than any previous technology. And then you see in super-microscopic print, "Please be sure to observe all the copyright laws of the land," in the tiniest of print in print ads, and it zips across the screen in the TV ads. It is clear that there is an intramural battle going on in the technology community.

And frankly, I think we in Government can no longer step to the sidelines.

At the same time, music companies have tried to give consumers what they what and, frankly, have done a crummy job. You know, I signed up for Pressplay a couple months ago, and the thing was loading and loading. And it has this icon that goes around that says, "Please wait while we load the program." And it was going for hours and hours. And finally, I called someone to find out what was going on, and they said, "Oh, you have Netscape. We don't work with that browser."

It is getting better. But at the same time the music companies are coming out with improved products to help consumers, Morpheus has another version out, KaZaA has a better version out. I

mean, there is a battle going on, a fullthroated battle going on not only between technologies but even within technology companies. I mean, if you have Sony who makes the computers and the downloaders and the minidisk players, and they're also producing music, it is not even clear the companies are on the same page about how to deal with this problem.

I have to confess that when I first heard about Mr. Berman's bill, I was, like, that's tough stuff, that I'm going to go and somebody is going to be scouring these peer-to-peer transactions and saying, "I don't like this guy. I'm going in there, and I'm going to stop this from happening." But I think it is evidence that I think the panel and those that listen to this hearing, it should be very clear that Congress is not going to sit in watch this go on much longer.

And I agree with, I believe it was Mr. Meehan, who said that no one has made a good argument to me about why this should be allowed to continue. No one has made a good argument to me about why my good friend Britney Spears is wrong, that you can't just go into a record store and grab what you like and say, "Well, the other 12 songs are crummy, so I'm going to grab this CD anyway."

You know, I believe that the industry obviously has to give consumers what they want. But I think it clear, whether you believe in the line-by-line explanation of the Mr. Berman's bill, it is clear that he reflects the sentiment of Congress and, frankly, I think of all moral American consumers that we cannot allow this pilfering to continue unabated.

I yield back the balance of my time.

Mr. COBLE. I thank the gentleman from New York.

And we've been joined by the gentlelady from Pennsylvania, who tells me she has no opening statement.

I thank the Members for your opening statements. I appreciate that.

And now we will get to the business at hand. Our first witness is Ms. Hilary Rosen, who is the chairman and chief executive officer of the Recording Industry Association of America, popularly known as RIAA, the trade group representing the U.S. sound recording industry. She was named president and CEO of RIAA in January 1998 having been with the organization for more than 11 years. Prior to joining the RIAA, Ms. Rosen operated her own consulting firm. She holds a bachelor's degree in international business from the George Washington University.

And by the way, folks, pardon my gravelly voice, but I am coming down with my annual autumn cold, so I know it sounds not favorable.

Our next witness is Ms. Gigi Sohn, who is the president and cofounder of Public Knowledge, a new nonprofit organization that will address the public's stake in the convergence of communications policy and intellectual property law. Ms. Sohn also served as executive director of the Media Access Project, a Washington-based public interest telecommunications law firm. Ms. Sohn holds a B.S. degree in broadcasting in film, summa cum laude, from the Boston University College of Communications and a J.D. from the University of Pennsylvania School of Law.

Our next witness will be Mr. Phil Galdston, who is a songwriter-producer whose work has appeared on over 60 million records

worldwide, in countless motion pictures, and on recordings by several famous artists. His song "Save the Best for Last," recorded by Vanessa Williams, simultaneously reached number one on Billboard's three major charts, and received four Grammy nominations, including song and record of the year.

Our final witness today is Mr. Randy Saaf, who is president and chief executive officer of MediaDefender Inc., makers of Internet and peer-to-peer anti-piracy software. Mr. Saaf attended the Harvey Mudd College School of Engineering in Claremont, California, and worked in software development at Raytheon Systems. At Raytheon, he helped to create more cost-effective solutions for developing radar software for the F–15 fighter jets.

It's good to have all of you with us. We have your written statements. They have been examined and will be reexamined, I assure you.

Again, folks—Hilary, you know this. You've been here before. I'm not sure the others have. But we would appreciate your confining your statement to the 5-minute rule, if you will. And you will know your time has expired when the red light before you illuminates into your eyes. [Laughter.]

Ms. Rosen, why don't we start with you?

STATEMENT OF HILARY ROSEN, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, RECORDING INDUSTRY ASSOCIATION OF AMERICA

Ms. ROSEN. Thank you, Mr. Chairman. And I'll submit my record statement for the record.

I have to join your colleagues, if I might, and add my personal and certainly our industry's respect and appreciation for your chairmanship. I think there are few legacies in this Congress, in many Congresses, that will match yours.

Mr. COBLE. Ms. Rosen, we may have to give you 10 minutes. [Laughter.]

Thank you, Ms. Rosen. I appreciate it.

Ms. ROSEN. The breadth of the creative output that results from the work that you've done coupled with I think the real balance you've achieved and strove for in technological innovation I think most importantly serves the public interest on all fronts. And I think the public has never been more satiated with creative works and the U.S. economy has never benefited more.

Congressman Berman, thank you for introducing this bill and stimulating this hearing on this extraordinary important problem.

America's copyright industries, it's always appropriate to remind this Committee and the public at large, account for over 5 percent of our Nation's GDP. Over the last 25 years, these copyrighted industries have grown at twice the rate of any other American industry, responsible for over 5 million jobs, provided the most favorable balance of trade to the U.S. economy than any other single industry, outpacing aerospace and agriculture in that regard.

The policies of this Committee to date have been responsible for that growth, and I urge you to continue that strong leadership.

Music is this first in this online piracy problem. Everybody knows it. We're getting a lot of attention lately, but every other copyright work, from needlepoint to books to film to software, will

be where are shortly, if we don't all pay more attention to this, because the economic engine that has driven these industries is at risk.

New business models in the legitimate online music market cannot compete. They are urgently threatened with the exponential growth of illegal piracy on peer-to-peer networks. The networks certainly impact equally on the security and safety of the users' own computers and their own private information, and that is in no way an indictment of the network itself. They're perfectly legal. It is the use of the networks that are most at risk. That certainly doesn't dissuade anyone from the notion that the concept of P2P and distributive computing has enormous commercial potential and enormous potential for consumers.

Finally, there really is no easy solution. There's no single bullet, as Mr. Keller sought. Frankly, I'm not even here to blame anyone, other than perhaps the network providers themselves who know exactly what they have created in order to profit on it.

Rather, self-help in the music business has been our internal mantra of late. And we have looked at that self-help in four different ways.

The first is business strategies. There is no substitute for giving consumers what they want. The record industry, it has been repeated multiple times, was slow to get there. But now there are legitimate services up and available. They clearly don't have as much music as the pirate services, because they don't have to worry about finding copyright owners to make sure that they get paid and are licensed. But they're there. And in fact, they are growing, and they're good music experiences today. They'll be better music experiences in several months. There are download services available now and already have been announced for significantly low prices; you know, less than a dollar a single. I think that that record of licensing over the last year speaks for itself.

The second strategy really are technical measures. We have to look at things like spoofing. The New York Times yesterday gave credit to spoofing for spurring the development of the legitimate marketplace, exactly what this Committee and what everybody should want to achieve.

Unfortunately, this week, we saw this announcement, that Sharman Networks in their new KaZaA download has decided that they're going to hamper spoofing. They can get away with technical measures against us, but all of this public outcry about technical measures to support ourselves.

So spoofing has been effective, but it is at risk. Because of this, we have to be able to keep up.

The second, obviously, is enforcement. I strongly believe the Federal Government has a role in enforcing criminal penalties. And the NET Act was an important step. The Justice Department has already announced their intention to be more aggressive in this area. They recognize the national economic threat, the national security threat. And we applaud that action.

On the civil enforcement side, we've taken a lot of self-help. We have been very aggressive, spent a lot of money, and sued a lot of networks. Those suits have generally been successful. The problem

is, there are just too many to consistently sue, and people have to understand that burden.

And finally, public education. We've done a lot of research over the last couple of months about consumers and attitudes and views about this practice and its impact on the marketplace and what consumers really need to hear. Since so much of the growth in peer-to-peer network use has been in the 12- to 18-year-old category—in fact, 18- to 30-year-olds, the activity has generally been about the same in the last 2 years. What we're seeing is tremendous growth in the 12- to 18-year-old. That means, as parents buy broadband and DSL and cable online services for their house, their kids are using that to go upstairs and steal music.

What people really wanted to know is, is it legal or not? And the courts have spoken: It's not legal.

What the music community has done this week is launch a public education campaign based on that specific area of education. We are telling people what their rights are. We're encouraging people to think about what playing fair is. And we're telling them when their behavior is illegal.

And this newspaper ad appears today in several national newspapers. It says, "Who really cares about illegal downloading?" And it's signed by 90 artists, most famous but some not so famous. The famous artists obviously trying to send the message on behalf of those young artists and coming-up artists that there is a long-term concern for the music community.

There is a Web site, MusicUnited.org. And this effort has brought together every single significant organization in the music community, many of whom this Committee has seen fighting among ourselves every day of the week on other issues. This issue unites us.

So I encourage people to take a look at this campaign over the next several weeks. You will have seen small retailers talk about this problem. You will see economists talk about this problem. You'll hear songwriters and fans talk about this problem. This is a serious problem, and this Committee bringing this problem to the public's attention is enormously important, so thank you very much for today's hearing.

[The prepared statement of Ms. Rosen follows:]

PREPARED STATEMENT OF HILARY ROSEN

Mr. Chairman, Representative Berman, and Members of the Subcommittee, I want to thank you for holding this important hearing today. This is the first hearing Congress has held to specifically examine the effects of copyright theft over peer-to-peer networks on the Internet.

And as a representative of the industry that has been so far the hardest hit by this enormous problem, I am deeply grateful to this Subcommittee for taking the lead in focusing on what is becoming an epidemic for the American economy and culture.

Just to give you an idea of the amount of copying that is occurring on unlicensed, free peer-to-peer systems—the most popular network, KaZaA, boasts on its site that its file-sharing software has been downloaded more than 120 million times. It is estimated that more than 2.6 billion files are copied every month—and no creator, no property owner is compensated for these copies.

I wish I could tell you that there is a silver bullet that could resolve this very serious problem. There is not. The answer resides in a combination of efforts that must be undertaken at the same time: 1) extensive public education about the illegality of file-sharing; 2) the widespread availability of licensed services that consumers desire; 3) criminal and civil enforcement; and 4) technological self-help

measures that prevent illegal copying and make it less desirable. These are all essential parts of assuring the vitality of our copyright system and the incentive to create new works.

We begin with education. Polls show that many Americans still do not know that downloading an artist's song on one of these unlicensed services is unlawful. And the message is clear—taking music on the Internet is no different than taking it from a store. The law protecting the right to reproduce a creative work applies on the Internet in the same manner in applies to sales of illegally made CDs on the street.

I want to emphasize that technology is not the enemy. Peer-to-peer technology holds amazing promise for creators and consumers to experience entertainment and to communicate in ways never before available. It is the misuse of technology—employing it to deprive compensation to creators—that must be tackled.

For the past two years, record companies have been working with download sites and new subscription services to create a legitimate alternative to piracy networks. There now exist dozens of places on the Internet to download authorized music and a dozen new competing on-demand monthly subscription services, all of which pay the creators. They are not yet perfect. In the legitimate world, it takes time to negotiate licenses in the free marketplace, to develop secure encryption and digital rights management systems, to negotiate with all rights holders, to develop new royalty payment systems, and to organize and digitize for new delivery our vast music catalogs. Pirate systems face none of these obstacles. While in Internet time it may seem like an eternity, in only three years we are well on our way to transforming an entire industry.

Enforcement of creators' rights is another key component. I want to thank all of the Members of this Subcommittee who signed a letter to the Department of Justice urging that they prosecute those who create systems intentionally developed to enable theft, and to prosecute those who intentionally steal through peer-to-peer services. And we applaud the Department for its recent announcement explaining that theft on these systems is no different than theft through a different medium—and that they will prosecute copyright crimes on peer-to-peer networks. In addition, in the civil courts, we have brought suit against the most popular peer-to-peer services for mass copyright infringement. We are pleased that the courts have ruled that services such as Napster and Aimster must be held accountable. The Judge in the Aimster case recently summed it up best when it said that Aimster "managed to do everything but actually steal the music off the store shelf and hand it to [its] users." We are hopeful that the courts will come to the same conclusion in the case we have filed, along with the movie studios and the music publishers, against KaZaA, Morpheus and Grokster. Enforcement alone, however, is not enough. We must be able to technologically prevent the illegal downloading of our creations over these systems.

That is why I also want to thank Representative Berman and cosponsors for introducing a bill that is intended to level the technological playing field by assuring that copyright owners can take preventive measures that will deny the downloading of their works when it is not authorized—without invading a user's privacy or damaging a user's computer or network.

An example of why it is so important to give copyright owners the ability to defend themselves with the same technological measures used by pirates to encourage theft came just this week when KaZaA announced that it was giving its users "better options and more tools than ever before . . . include[ing] a filter to help users avoid . . . misnamed or incomplete files that may have been uploaded by record labels and copyright owners trying to frustrate file sharing.' It is truly ironic that we can be stopped from trying to protect ourselves against unlawful copying by technology, but using technology to prevent unlawful use is met with a firestorm of controversy. It is also ironic that KaZaA can employ a filter to avoid spoofed files, but not to filter out copyrighted works to which they have no right.

Unfortunately, there has been a lot of misinformation about this bill. Some have characterized it as allowing copyright vigilantism, or letting record companies and movie studios hack into people's computers, and crash networks. These irresponsible descriptions at best reveal a misunderstanding of the text and purpose of the bill, and at worst purposely cloud the real issues and problems with unlicensed peer-to-peer networks. It is the use of a peer-to-peer system that opens up a user's hard drive to the rest of the world, not the Berman bill. It is the current practice of those who have created today's unlicensed peer-to-peer systems that invade a consumer's privacy through spyware and the selling of consumer information, not the Berman bill. In fact, the bill prevents these activities, along with hacking, deleting or altering material, and causing damage to a computer. We support these prohibitions and other solutions to assure that all privacy and damage concerns are addressed. But

we ask that those who share these concerns with us help us to come up with real solutions that also curtail massive piracy over these networks.

The intent of the bill, it seems to us, is simply to allow a copyright owner to prevent the initial downloading on a peer-to-peer system of specifically identified material that it owns. An analogy might be a U.S. Coast Guard boat that is out in the sea preventing unlawful goods from entering the United States. It is not doing damage to the sender or the intended recipient, it is not boarding any other boats, or initiating any harm. It is simply acting in a defensive manner to block admission and to deny an illegal transfer. In our opinion, this preventive activity is warranted and necessary.

Many of these types of activities are already allowed under current law, and copyright owners are availing themselves of their rights to protect their works. But some laws that were written at a time when peer-to-peer networks were not even contemplated have created some unintended confusion and ambiguity. It is sort of like a statute that was written to protect bank statements in the 1950s being applied to measures utilized to protect ATMs today. The Berman bill will clear up any uncertainty in both the application of current law and the respect that copyright owners must and should have for the integrity of networks and an end user's privacy.

We, like others, have many questions about the application, scope and exposure to copyright owners in the bill. But we are committed to working with the Subcommittee to resolve these questions and to work with those who have raised other legitimate concerns.

And we are also committed to working with all parties who have a stake in creating a legitimate digital marketplace that will continue to make possible the gifts that music has brought to listeners around the world.

I would like to close, Mr. Chairman, by noting that, because of term limits, this may be the last time that our industry has a chance to formally appear before you as Chairman of this Subcommittee. To call your tenure as Chairman extraordinary in the formation of modern copyright law would be a gross understatement. Your leadership is responsible for future creations that we have not even imagined. And your legacy is appreciated by all of us who are involved in the creative arts. We salute you and thank you.

Mr. COBLE. Thank you, Ms. Rosen. And thank you for your generous comments as well.

With a sense of fairness, Ms. Rosen consumed 7 minutes, so I will allot each of you 7 minutes as well.

So, Ms. Sohn?

STATEMENT OF GIGI SOHN, PRESIDENT, PUBLIC KNOWLEDGE

Ms. SOHN. Thank you, Chairman Coble, Congressman Berman.

Mr. COBLE. If you will suspend, Ms. Sohn, you don't have to use 7, but you may use 7. [Laughter.]

Ms. SOHN. I think I probably will.

Thank you, Chairman Coble, Congressman Berman, and the Members of the Subcommittee for holding this very important hearing. I am honored that you've chosen me and my organization to represent the consumer perspective on P2P networks.

We share your concern about massive illegal file sharing over P2P networks. We condemn such actions and favor targeted mechanisms to limit them. I emphasize the word "targeted." We cannot support laws or technological measures that harm legal uses of computers and the Internet.

Unfortunately, H.R. 5211 is not a targeted measure. We recognize and appreciate the good intentions of Congressman Berman and the other co-sponsors in attempting to limit unlawful file sharing over P2P networks. But this bill would permit copyright owners to employ self-help technological measures at the expense of all Internet users, whether or not they're engaging in illegal activity and whether or not they're using the type of P2P networks that are the purported subject of this bill. It is especially troubling that

these measures can be employed secretly without any notice to the affected consumer as to who is engaging in self-help or why.

Let me tell you what concerns us. One technique, interdiction, involves a program robot, or bot, that repeatedly requests an allegedly infringing file a P2P user, making her hard drive inaccessible. Sounds benign? Well, what if the bot is just wrong about whether a file is illegal?

The content industries say that their bots are accurate. But when Warner Brothers twice asked an ISP to disable access for a file trader that had a 1k file named "harry potter book report.rtf," did it really believe that such a small text file was anything but a child's homework?

And remember, the rights in this bill redound to all copyright owners. So while the content industries may have the means to use more expensive and accurate self-help, others will use whatever homebrewed tactics they can afford.

And what if these or other future self-help techniques result in file trader's computer crashing or her Internet service becoming unavailable? Regardless of whether an individual has an infringing file, denial of service caused by self-help will burden ISPs and other network users. Every denial of service claim requires ISP time and resources to figure out its source, causing it to spend less time on other more serious service problems.

Moreover, denial of service attacks on ISP networks using shared architecture could directly affect the service quality of other ISP customers.

The anti-consumer effects of this bill do end there, unfortunately. Even in the unlikely event that an innocent victim of self-help can figure out who among the millions of copyright owners is responsible, the bill erects economic and procedural barriers to seeking relief in the courts. This is true even the when the copyright owner's actions are the most egregious.

These obstacles and the broad authorization granted to copyright owners under this bill shift the burden of using self-help away from the content industries and places it squarely on the backs of consumers.

What H.R. 5211 could sanction is a virtual Wild West. Attacks on hard drives will likely provoke retaliation by some users and the acquisition of defensive software by others. The collective impact of all these efforts might be to reduce or eliminate the effectiveness of the Internet and delay the rollout of broadband.

So if H.R. 5211 is not the right answer, what is? I recommend four solutions, all of which are currently available to content industry.

One, enforce existing laws. This is the ultimate self-help technique. We are not aware of one case in which the recording industry has taken legal action against an individual downloader. The problem is that the industry apparently does not want to enforce the law when it comes to illegal file trading because it looks bad to sue its own customers. But it's not Congress' job to protect any industry from negative public relations.

Two, employ noninvasive self-help. We support the use of self-help techniques that are activated by an individual's affirmative ef-

fort to obtain an unlicensed copy of a file, including spoofing, flooding, decoy, and redirection.

Three, promote competition to build a new business model. There appears to be a growing consensus that online music services that provide easy access to a wide range of high-quality content at a fair price can compete with free. The New York Times reported yesterday that more and more file traders are using legal online music services in part because file sharing is, in the words of one convert, a dreadful experience. In fact, Jupiter Research predicts that by 2006, the industry will reap more than $1 billion from these services. Forrester Research puts that estimate at $2 billion.

But more can be done to expedite a better business model for selling music online. One way is for the recording industry to give others the opportunity to sell music online, not for free. The record companies could license their music to online retailers and ask for the same statutory rate that the publisher gets for each song sold.

This is a win-win situation. The copyright owner gets paid, and a competition ensues to build a viable online music service. The Music Online Competition Act, which is currently pending before you, is an important step in the direction of increasing competition in the lawful delivery of online music.

Four, educate the public about digital copyright. I applaud the recording industry on the educational campaign it has started today. The content industries have some of the world's biggest and best public relations capabilities. They should use them to give the public truthful information about what is legal and illegal in a digital world.

I want to again thank Chairman Coble, Congressman Berman, and the Members of the Subcommittee. As the sole representative of citizens' rights at this hearing, I respectfully ask that you keep the record open for 30 days to permit others to submit testimony and comments.

[The prepared statement of Ms. Sohn follows:]

PREPARED STATEMENT OF GIGI B. SOHN

Chairman Coble, Congressman Berman and other members of the Subcommittee, my name is Gigi B. Sohn. I am the President of Public Knowledge, a new nonprofit public interest organization that seeks to ensure that citizens have access to a robust public domain, an open Internet and flexible digital technology.

I want to thank the Subcommittee for holding this important hearing on the great promise of peer-to-peer (P2P) networks and some of the perils associated with their use. I am honored that you have chosen my organization to represent the citizen/consumer perspective at this hearing.[1]

My hope is that this hearing will further advance the dialogue that Public Knowledge and other public interest organizations have already begun with the various interested industries and with policymakers. That dialogue is intended to find solutions that provide the content industry with a "reasonably secure" digital environment for its content while ensuring that citizens retain their rights under copyright law and continue to have access to an open Internet and the kind of flexible technology that they have come to expect and enjoy.

P2P TECHNOLOGY IS CHANGING THE FACE OF COMPUTING—FOR THE BETTER

In just two years, P2P has become a computing phenomenon. Millions of Internet users are communicating with each other through P2P file sharing software programs that allow a group of computer users to share text, audio and video files stored on each other's computers. While the P2P applications we know today are just a few years old, the technology underlying P2P is at the heart of the Internet.

The Internet was designed to be a distributed system of linked computers in which users could freely share content and data stored on each other's computers.

Few disagree that P2P networks are already changing the way businesses, educators, artists and ordinary citizens use their computers. In businesses, for example, they offer an alternative to centralized server-based sharing of documents and projects. [2] The vast majority of these changes are positive. By linking together individual computers and distributing their power, P2P technology is superior to the centralized server approach because it:

- is more robust and resilient
- is more cost effective
- is faster and more reliable
- harnesses bandwidth and storage resources that would otherwise go unused
- enables real-time collaborative work

Already, both public and private P2P networks are helping small and large businesses (including content companies), universities, artists and others work collaboratively and more efficiently. Here are some examples:

- The University of North Carolina at Chapel Hill. Robert Kirkpatrick, Distinguished Associate Professor of English and Director of the London Summer Honors Program at the University of North Carolina at Chapel Hill, used Groove Network's P2P tools to manage a class in the composition of poetry. Among other things, Kirkpatrick used P2P technology to encourage collaborative editing and comment on students' work, adjust the syllabus, archive course materials, and create a list of links to resources of poetic forms and vast archives of complete works of poems and critical writing. The class also uses the Groove tools for a class forum and an announcement board to share information on musical, dramatic and other events on campus. Kirkpatrick said that P2P technology "makes it possible to extend that most expensive form of education—one-on-one tutorial—into a cohesive class experience. . . . It comes very close to being, for me, the ideal academic tool." [3]
- CenterSpan. CenterSpan is a distributed content delivery network licensed to distribute copyrighted digital content from major media companies. Earlier this year, CenterSpan announced an agreement with Sony Music Entertainment whereby CenterSpan's secure P2P network provides music from Sony Music artists to a wide variety of online service providers seeking to offer their subscribers streaming and downloadable music. [4]
- J!VE Media. J!VE Media is the creator of a suite of digital video packaging, digital rights management and media delivery services which enable content providers to distribute protected digital video content via publicly accessible P2P networks, including the Gnutella Network (which includes users of LimeWire and Morpheus) and the Fastrack Network (which includes users of KaZaA and Grokster). J!VE uses P2P distribution technology because it allows content owners to rely almost entirely on users to provide the most costly computing resources involved in digital distribution: data storage and bandwidth. J!VE distributes only authorized content, and its customers include: 1) the Priority Records division of the EMI Recorded Music Group; 2) Koch International, the world's third largest independent music label; and 3) The Comedy Network, Canada's 24 hour comedy cable channel. [5]
- Project Gutenberg. Project Gutenberg seeks to convert to ebook form, and widely distribute over the Internet, over 4500 works from the King James Bible to Shakespeare to the CIA World Fact Book. These works are either in the public domain or authorized by copyright owners for distribution. One of the chief hurdles facing Project Gutenberg and public domain projects like it has been the expense of hosting and distributing the resulting files. Today, these expenses are being reduced, and valuable public domain works are reaching more people, because these texts are being distributed over P2P networks. [6]
- Furthur Network. The Furthur Network is a non-commercial, open source, P2P network of legal live music. Music lovers download and share music from each other. Musicians that allow the non-commercial taping and trading of their live performances are allowed on this publicly accessible P2P network. This would include bands like the Grateful Dead, the Allman Brothers Band and the Dave Matthews Band. TDK, the consumer electronics and recordable media company has recently recognized the importance of this segment of the music industry by sponsoring the third annual Jammy Awards, which honors

musicians who focus their art on live music. In the words of Bruce Youmans, TDK's Vice President of Marketing, "There are literally hundreds of sources, including directly from some of the artists performing at the Jammys, for legally acquiring today's best music without infringing on artists' copyrights." [7]

All indications are that P2P technology will stimulate our economy if it is allowed to flourish. As with any successful new technology, innovators will seek to capitalize by developing new applications for P2P. [8] Moreover, since every computer on a P2P network becomes, in effect, a file server for every other computer, it is likely that businesses and individuals will demand faster and more powerful PC's. Equally as important, many experts predict that increased use of P2P networks will drive up the demand for broadband. [9] It is not difficult to see why—using the increased bandwidth capabilities of a P2P network, a homeowner using only a DSL line could send files at a speed and capacity that is eight times faster than a T-1 line!

LIKE OTHER TECHNOLOGIES, P2P CAN BE ABUSED

Despite the recognition of Congressman Berman and other legislators of the enormous promise of P2P networks, [10] the focus of this hearing is on their abuses—that is, the illegal sharing of copyrighted material over these networks. Let me be clear—Public Knowledge does not condone the illegal sharing of files on any network—be it P2P or otherwise. We believe in the constitutional and historical purpose of copyright protection, that is, to encourage the creation of new artistic works for the ultimate benefit of the public. That purpose is not well served by individuals who engage in large scale illegal file trading. As discussed below, we think that the content industry has several avenues available to it to curb these abuses that will also preserve the technology and the rights and expectations of consumers and computer users.

That being said, my fear is that the emphasis on the abuses of P2P networks may well give rise to actions that could ultimately destroy the promise of this technology. As discussed below, proposed laws like H.R. 5211 could lead to actions by copyright owners that could literally bring these and other networks to a sudden and unfortunate halt. Even where the copyright owner's motives are the most benign, actions authorized by this bill could seriously tax these valuable networks by making them less efficient, more unstable, and subject to greater private control. That is not good for consumers, the tech industry or the content industry, which believes, as I do, that it will figure out how to harness P2P technology and profit. Thus, it is not just the illegal activity that might be slowed by the kinds of self help techniques authorized by this bill, but also every legitimate current and yet-to-be-developed business dependent upon the promise of P2P technology.

P2P networks, like other technologies (e.g., cars, telephones) can be used for good, or they can be abused. But we don't outlaw these technologies or limit their legitimate use because of the possibility (and yes, even the probability) that someone will use them to do harm. Public Knowledge supports targeted mechanisms to limit abuses of these networks. But we cannot support laws or technological measures that harm legitimate uses of the technology in the effort to curtail illegitimate ones.

THE CONTENT INDUSTRY HAS TOOLS AT ITS DISPOSAL WHICH, IF USED TOGETHER, CAN LIMIT THE IMPACT OF ILLEGAL FILE TRADING OVER P2P NETWORKS.

Over the past several months, my staff and I have had a number of productive conversations with various sectors of the content industry. While we have not agreed on everything, I have appreciated their willingness to be candid and engage in a continuing dialogue. One thing the various sectors of the industry have been willing to admit is that infringement cannot be stopped completely. This is true with regards to physical infringement as well as virtual infringement.

Thus, the critical question becomes: how can the effect of illegal file trading over the Internet be limited without eroding the legitimate consumer/computer user rights and expectations? I propose a combination of three tools:

ENFORCEMENT OF EXISTING LAWS

Both the Copyright Act and the Digital Millennium Copyright Act provide for remedies for certain unlawful uses of copyrighted material. [11] There is little evidence and indeed, the content industries do not claim, that when the law is enforced it is ineffective. In fact, when the content industries choose to enforce their rights under these laws, like in the Napster, Audiogalaxy and Madster (aka "Aimster") cases, they have succeeded.

Despite its claims that billions of songs have been illegally downloaded, we are not aware of a single case in which the recording industry has taken legal action against an individual downloader. The problem is that the recording industry apparently does not want to enforce the rights it claims when it comes to illegal P2P file trading because it looks bad to sue its own customers. Therefore, the industry has decided instead to shift that burden onto other corporations, and in particular, ISPs. As many of you know, the RIAA is seeking to force Verizon to hand over the names of its customers based solely on the RIAA's allegations that those customers are engaging in infringing activity. Verizon, backed by civil liberties and other public interest organizations such as my own, has argued, among other things, that forcing ISPs simply to give copyright owners the names of their customers without a judicial determination that they may be engaged in any illegal conduct would violate the constitutionally mandated privacy and anonymity rights of their customers, and put ISPs in the untenable position of having to respond to the numerous identification requests that would inevitably result.

Were Verizon and other ISPs to comply with such requests, the RIAA would be empowered to collect sufficient information with which to conduct investigations of potential defendants and engage in surveillance over a period of days or even years, choosing to sue the defendants presenting the worst facts and having profiles least likely to garner public or judicial sympathy. As is often said, bad facts make bad law. The RIAA plan appears to have no other purpose than to find the worst facts before seeking an interpretation of its legal rights.

Verizon's refusal to succumb to the RIAA's request does not leave the industry without a remedy. It can bring a "John Doe" lawsuit against anonymous infringers and serve Verizon with a third-party subpoena pursuant to Fed. R. Civ. P. 45. Once the industry has satisfied a judge that its allegations of infringement have evidentiary support, Verizon (and other ISPs) will be required to make available those names. With "robot" technology that allows the industry to pinpoint the most egregious uploaders with some (but by all means not perfect, see discussion below) accuracy, the industry's complaint that it would have to bring numerous expensive lawsuits rings hollow. Unless the industry wants to sue every person with a handful of infringing files on its hard drive, it has the economic and technological means to locate the kind of large scale alleged infringer that it would want to bring to court.

An industry-initiated law suit against a large scale infringer could also have the benefit of serving as a deterrent to other bad actors. As we have seen in other contexts, specifically targeted lawsuits and other legal action can have a deterrent effect, and also educate the public as to what is legal. But if the industry refuses to bring targeted cases, we will only be left with unfounded complaints that the copyright law provides a "right without a remedy." The remedies exist, but copyright owners must take up the challenge of invoking them.

NON-INVASIVE SELF-HELP

Public Knowledge does not oppose the use of reasonable non-invasive self-help techniques by the content industry. By non-invasive, we mean techniques that do not entail a third party attacking a file located on a computer hard drive (or denial-of-service attacks on individual users or on providers). Examples of non-invasive self-help include spoofing, flooding, decoy, spoiler files and redirection. Many of these techniques involve the intentional distribution of phony or corrupted files that an individual seeking to make an unlawful reproduction will then download. Others will send downloaders to legitimate sites. What distinguishes these techniques is that they are activated by an individual's affirmative effort to obtain an unlicensed copy of a file.

On the other hand, Public Knowledge cannot support self-help techniques that permit the copyright owner to block access to an individual's computer hard drive for the purpose of making an allegedly illegal file unusable or incapable of being downloaded. In the most popular of these techniques, commonly known as Interdiction, a computer program repeatedly requests the same file from a particular P2P network user. As a result, no one else can get to that file, or to any other file on that user's computer even if the other files to which access is sought are perfectly legal and downloading them is perfectly lawful.

There are several problems with self-help techniques of this kind. The first, of course, is that the program, or robot, could be mistaken in its determination that a file is one that warrants protection. While we have received assurances from the RIAA that the "bots" that its member companies use are extraordinarily accurate, evidence submitted in its pending litigation with Verizon demonstrates otherwise. For example, UUNet, an ISP, was sent a notice by Warner Brothers, owner of the

copyright to the motion picture "Harry Potter and the Sorcerer's Stone." The notice asked UUNet to disable access to a user, identifying as the single infringing file a 1K file named "harry potter book report.rtf." The size and type of the file make it clear that the file was nothing more than a child's school book report on a Harry Potter book. The record includes other examples of similar inaccuracies.[12]

Moreover, it is important to remember that the members of the RIAA will not be the only copyright owners capable of using these techniques, particularly if H.R. 5211 becomes law. The fact that Interdiction not only makes unavailable the allegedly infringing file, but also makes the rest of the user's files unavailable only exacerbates this problem.

A second concern is that Interdiction and similar self-help techniques punish individuals for "making available" copyrighted content, regardless of whether that content was legally obtained or not. Such punishment would extend copyright protection beyond what the law currently allows. Unlike in the European Union, U.S. copyright law does not give a copyright owner a separate right to "make available" his work. Efforts to include such a right here have been heretofore rejected.

Finally, we are concerned with the worst case scenario—that repeated requests or similar actions could prevent a user from accessing the Internet for any other purpose, resulting in a so-called "denial of service." Regardless of whether an individual has an infringing file, denial of service caused by self-help will burden ISPs and other network users, both indirectly and directly. This is particularly true where such attacks can be done secretly, such that a user's first call will be to its own ISP to complain about a malfunction. Even on a network where a loss of service for one may not directly affect other users, every denial of service claim requires ISP time and resources to figure out its cause, causing it to spend less time on other, more serious service problems, which might be caused by cyberterrorism, other security breaches or legitimate technological breakdowns. This has an indirect effect on all the other customers on an ISPs network and also burdens the entire network. Moreover, with some ISP networks (particularly the shared architecture of cable modem service), the service quality of innocent ISP customers could be directly affected if invasive self-help leads to a denial of service for another customer—in other words, innocent ISP customers are harmed by the acts of one suspected infringer.

Legitimizing and harboring invasive self-help has startling implications. Again, whether the large content companies use techniques that are more accurate and often unrecognized by the computer user is nice, but is largely beside the point. If expressly permitted or protected, self-help of various shapes and sizes will be available to all copyright owners, some of whom may believe that it is perfectly within their rights to launch denial of service attacks. Some of these attacks may affect actual infringers, while some almost certainly will affect innocent parties, who will have no idea why they (or others) cannot access their files or why their Internet service is not working. These attacks will likely provoke retaliatory attacks by some users, and the acquisition of defensive software by others. Soon, the Internet will look like the Wild West, with self help bots and bot blockers replacing guns as the weapon of choice.

The collective impact of all these self help efforts, particularly if they are sanctioned by law, might be to reduce or eliminate the effectiveness of the Internet as a communications medium in a number of ways, from consuming bandwidth to forcing ISPs into imposing crippling terms-of-service agreements. The final victim of this Internet free-for-all, of course, would be rollout of broadband, for which P2P is the "killer app."

PROMOTING COMPETITION TO BUILD A NEW BUSINESS MODEL

Last June, at the request of USA Today, I spent several hours discussing digital media issues with a number of top executives from the content and consumer electronics industries. What struck me was that the New York representatives of the content industries all agreed on one thing: that they had to create new business models that take advantage of the low cost, ubiquity and speed of the Internet. In answering the question of whether the recording industry had responded to the Internet needs of its customers, John Rose, Executive Vice President of the EMI Group stated:

There's no question that this industry, like every other industry that went through this, didn't deal with it in as forward-thinking a manner as it could have. The real question is: here's where we are, what do we do about it? There's no way you're going to constrain the Internet, . . . The question is, can you come up with economic models to empower guys like Alan [McGlade of MusicNet, an industry-backed online music service]?[13]

These content industry executives believe, as I do, that if they can provide easy access to a wide range of high quality content at a fair price, most consumers looking for content over the Internet will choose their services.[14] In other words, they believe that they can, in fact, "compete with free."[15] Rob Reid of Listen.com, an online subscription music service that licenses music from the recording industry, said as much in a recent Department of Commerce Forum:

The way I compete [with free] is I have to create a service that's better than free, which is hard to do. I mean, that's hard to do. I mean, that's a tough proposition, but the good news is people do opt for things that are better than free all the time. If they didn't, you know, we'd be eating at soup kitchens every night, and not going to restaurants. And just looking around this table, I see a bottle of Poland Springs . . . that tells us that designer water is a multi-billion dollar industry, and that comes out of the faucet for free. So better than free does exist.[16]

Despite the fact that industry efforts to bring content online have been going on for years, a successful business model has not emerged. One of the reasons this is so is that creating such a model is not a simple task—it takes time, resources and sometimes plain dumb luck.[17] But I believe that there are two other reasons a business solution has been slow in coming: 1) the same industry minds have been attacking the same problem for all that time, and 2) the industry has refused to permit others to try and figure out how best to deliver content over the Internet.

If the content industries are sincere in their desire to create new business models (and I believe that they are), then they should give others the opportunity to help them to do so. Not for free—for example, the recording companies could license their music to various online retailers and ask the licensee for the same statutory rate that the publisher gets ($0.08) for each song the licensee sold online. Retailers who choose to offer them to the public must all pay the same "wholesale" price but can then compete vigorously with each other to find the business proposition most appealing to consumers. This is a win-win situation. The copyright owner gets paid, and a competition ensues to build an online music service that provides a high quality, large catalogue at a reasonable price. In fact, several successful business models could emerge that are entirely different than anything being contemplated today and appeal to different types of consumers, just as retail stores do for pre-packaged goods. There will be failures, no doubt—but until innovators and entrepreneurs are given a chance to fail, the chances that success will be achieved are greatly diminished, and the public benefit from broad and competitive dissemination will surely be lost.[18]

H.R. 5211 IS A WELL-INTENTIONED BUT FLAWED BILL

Public Knowledge appreciates the good intentions of Reps. Berman, Coble, Smith and Wexler in sponsoring H.R. 5211. We believe that they are sincere in their desire to encourage P2P technology and to stem the flow of illegal file sharing.

Unfortunately, these good intentions cannot save this flawed bill. Part of the problem is that because P2P technology underlies the entire Internet, it is difficult to draft legislation that addresses specific P2P networks such as Morpheus and KaZaA without also including the entire Internet and World Wide Web in its scope. Also, as discussed above, it is difficult to imagine certain "self-help" techniques that could interfere with specific P2P networks that would not also put the efficient functioning of the larger Internet at risk, impose enormous new tech support burdens on ISPs and impair customer satisfaction with broadband. Finally, as discussed above, while we may accept that some of the techniques now in use by the content industries are somewhat benign, this bill allows for self-help by all copyright owners—some of whom may not have the same concerns about upsetting their customers as do large content companies.

Among the provisions in this bill that are the most troublesome from a consumer perspective are:

- The bill gives copyright owners extraordinary powers to engage in self-help. H.R. 5211 grants copyright owners and their agents the right to break any law, state or federal, civil or criminal, in furtherance of "disabling, interfering with, blocking, diverting or otherwise impairing" the availability of his or her copyrighted works on a public P2P network. This extraordinary power is limited by five vague conditions: 1) the copyright owner may not "alter, delete, or otherwise impair the integrity of any computer file or data residing on the computer of a file trader" (Subsection (a)); 2) the owner must not impair the availability of files on a targeted computer other than the works the copyright owner owners except as "reasonably necessary" (Subsection (b)(1)(a)); 3) the copyright owner may not cause "economic loss" to any person other than the targeted file trader (Subsection (b)(1)(B)); 4) the copyright owner may not

cause "economic loss of more than $50" to the targeted file trader (Subsection (b)(1)(C)); and 5) the copyright owner must notify the Attorney General seven days before engaging in self-help (Subsection (c)).

These conditions leave the door wide open for abuse by the copyright owner and harm to computer users. For example, the limitations on altering and deleting files in subsection (a) conceivably would not prevent a copyright owner from cutting a user's DSL line or even his phone line, or knocking his satellite dish off his roof. The "as reasonably necessary" language of subsection (b)(1)(a) is undefined and invites a raft of excuses for why an individual's non-infringing files were impaired by self-help. The subsections prohibiting "economic loss" do not cover any non-economic loss that a target file trader or innocent victim may incur. And Subsection (c)'s notice provision is toothless: there is nothing in the bill that gives the Attorney General guidelines by which to judge self-help techniques or the power to reject them. All that is required by that subsection is notice.

- The bill shifts the burden of using self-help mechanisms onto the consumer. Currently, the content industries are very careful about the type of self-help techniques they use. This is not only for public relations reasons—the misguided use of these techniques that harms an innocent party could also result in serious legal liability for a copyright owner. By providing a safe harbor for a whole range of non-invasive and invasive self-help techniques, H.R. 5211 removes the incentives and sanctions that currently impel content owners and others to be careful in their self-help. While the damage limitation for bringing a legal action for misguided self-help is only $250, copyright owners know that most victims will never sue because it is not worthwhile to do so; the damage rarely will be large enough to justify the time and cost of litigation.[19]

Equally as troubling is the fact that the bill creates no obligation for the copyright owner to notify a victim that her Internet access has been impaired. If they are subject to misguided self help, the vast majority of computer users will have no idea why their computer has broken down or why they can no longer access certain files. Without a notice requirement, even a tech-savvy victim who figures out what has occurred and decides to bring a lawsuit will not likely know whom to sue. Only if the victim can figure out exactly who impaired her system (among millions of copyright owners) can she then ask for the reasons for that action. Subsection (c)(2)(A).

- The bill erects enormous procedural obstacles for a victim of self-help to overcome before she can seek the remedies provided. H.R. 5211 creates a new cause of action for an affected file trader when a copyright owner "knowingly and intentionally impairs . . . [a] particular computer file . . . and has no reasonable basis to believe that such [file] constitutes an infringement of copyright," and also causes over $250 dollars in damages to the file trader. But where H.R. 5211 giveth, it also taketh away. Even though the copyright owner is engaging in egregious and willful activity, the bill erects procedural hurdles to innocent citizens seeking to obtain restitution for wrongful self-help. The innocent file trader cannot get to the courtroom without first getting permission from the Attorney General (Subsection (d)). Whether the victim will ever get to court is left to the sole discretion of the Attorney General, who has four months to make that determination. This creates a supreme irony: the bill erects huge legal barriers for citizens seeking remedies for misguided self-help, while it dismantles them for content companies seeking remedies for infringement. This is not only anti-consumer, it is also likely unconstitutional. It delegates to the Executive Branch the discretion to block civil litigants from access to federal courts, and delegates to private parties the power to do what no government can; namely, to surreptitiously impose a prior restraint upon communications that are presumptively protected by the First Amendment without any judicial determination that the speech being suppressed is unlawful.
- The bill expands protection for copyrighted works beyond that required by the Copyright Act. Subsection (a) of the bill provides a safe harbor for self-help actions that impair the "unauthorized" distribution, display, performance or reproduction of a copyrighted work on a publicly accessible P2P network. But not all "unauthorized" uses of copyrighted works are illegal under the Copyright Act. In addition, as discussed above, by permitting self-help against individuals who merely make works available (rather than just those who illegally download available works), the bill gives copyright owners an additional "right to make available to the public." This right is now only recognized by

European intellectual property laws, and has heretofore been rejected in the U.S.

H.R. 5211 is well intended to stem the flow of illegal file trading, but it goes way beyond what is necessary to permit the content industries to engage in the type of non-invasive self-help described above. While Public Knowledge might consider supporting a narrowly-crafted proposal that clarifies that non-invasive self help is permissible, H.R. 5211 is not that bill.

CONCLUSION

In conclusion, I want to thank Chairman Coble, Congressman Berman and the other members of the Subcommittee for holding this hearing to discuss P2P networks. As the sole representative of consumer and citizens rights at this hearing, I would respectfully ask that you keep the record open for thirty days to permit other public interest organizations to submit testimony and comments.

Public Knowledge urges the Subcommittee to act cautiously before seeking to alter the nature of a technology that improves the already significant abilities and flexibility of computers and the Internet, benefits artists, educators and businesses, and may very well be the "magic bullet" that drives broadband adoption. Illegal file trading on P2P networks can be limited through a combination of rigorous enforcement of the law, non-invasive self help techniques and promotion of competition to build new business models for online music. H.R. 5211, however, goes far beyond what is necessary or reasonable to limit illegal file trading, and if passed, could lead to actions by copyright owners that could threaten the core capabilities of the Internet.

Thank you.

Notes

1. Public Knowledge is working in partnership with the Center for Democracy and Technology and Consumers Union on P2P and related digital copyright issues.
2. A recent Gartner Research Note (Technology T–16–2550, September 16, 2002) predicts that "[b]y 2005, 10 percent of business interactions will occur via P2P-enabled technologies (0.7 probability)."
3. www.groove.net/solutions/testimonials/education/unc.html
4. Statement of Frank G. Hausmann, Chairman and CEO Centerspan Communications Corporation before the House Judiciary Committee Subcommittee on Courts, the Internet and Intellectual Property, June 5, 2002.
5. Declaration of Sean Mayers in Support of MusicCity.Com Inc.'s and MusicCity Networks, Inc.'s Motion for Partial Summary Judgment in MGM Studios v. Grokster, www.eff.org/IP/P2P/MGM—v—Grokster/20020122—mayers—decl.html
6. Declaration of Gregory Newby in Support of MusicCity.Com Inc.'s and MusicCity Networks, Inc.'s Motion for Partial Summary Judgment in MGM Studios v. Grokster, www.eff.org/IP/P2P/MGM—v—Grokster/20020122—newby—decl.pdf.
7. www. furthurnet.com
8. One exciting P2P application that is in its nascent stages is "P2P signing" for the deaf and hard of hearing. Through this application, an interpreter in one location can use high-speed communications and low-cost video cameras to provide interpreting services to consumers at other locations across the country. Frank G. Bowe, Broadband and Americans with Disabilities at 2 (2002), www.newmillenniumresearch.org/broadband.html.
9. Amy Kover, Napster: The Hot Idea of the Year, Fortune Magazine, June 26, 2000. See also, Understanding Broadband Demand, A Review of Critical Issues, Office of Technology Policy, U.S. Department of Commerce at 16 (September 23, 2002), www.ta.doc.gov/reports/TechPolicy/Broadband—020921.pdf
10. Speech by the Honorable Howard L. Berman to the Computer and Communications Industry Association Regarding Solutions to Peer to Peer Piracy (June 25, 2002), www.house.gov/berman/p2p062502.html ("P2P networks represent as much of an opportunity as a threat to copyright creators. P2P represents an efficient method of information transfer, has the potential to greatly reduce the costs associated with server-based distribution systems, and can support a variety of legitimate business models.")
11. 17 U.S.C. §§ 501–507; 17 U.S.C. §§ 1201–1204; 18 U.S.C. §§ 2318–2319A.
12. Motion for Leave to File and Brief Amicus Curiae of United States Internet Service Provider Association in Support of Respondent filed in Recording Industry Association of America v. Verizon Internet Services, Case No. 1:02MS003323 at 6–12.
13. "Digital Technology, Reshaping Industries, lifestyles," USA Today, June 25, 2002 at 4E.
14. The Office of Technology Policy at the U.S. Department of Commerce apparently agrees, Understanding Broadband Demand, A Review of Critical Issues, Office of Technology Policy, U.S. Department of Commerce at 17 (September 23, 2002), www.ta.doc.gov/reports/TechPolicy/Broadband—020921.pdf ("There is considerable belief that creative, legal, for-profit sites can out-compete 'free' alternatives. Industry will need to develop technologies that can protect digital content, ensure that legal services have the resources . . . to outcompete illegal exchanges, educate consumers about the need to respect intellectual property on the Internet, cooperate across sectors and deliver content in ways and on platforms that consumers want. . . .")

15. Bon Jovi and its record company, Vivendi Universal SA's Universal Music Group, is competing with free by giving fans who buy their CDs "Bon Jovi Exclusives," including preference in buying concert tickets, the possibility of climbing on stage and other band-related perks. Jennifer Ordonez and Charles Goldsmith "Bon Jovi Uses 'Bounce' To Battle Music Pirates," Wall Street Journal, September 16, 2002, online.wsj.com/article—print0,,SB103211681937801835,00.html.
16. Statement of Rob Reid, Founder and Chairman of Listen.com, Understanding Broadband Demand: Digital Rights Management Workshop, July 17, 2002, U.S. Department of Commerce, Technology Administration www.ta.doc.gov/reports/TechPolicy/DRM–020717.htm
17. A recent New York Times article details the challenges faced by online music services (including those backed by the recording industry) in getting permission to sell certain songs over the Internet. Amy Harmon, "Copyright Hurdles Confront Selling of Music on the Internet," NY Times, September 23, 2002 at C1.
18. This week's announcement by the Warner Music Group that it would begin selling digital singles starting at 99 cents through retailers like Bestbuy.com and MTV.com is a good start. Amy Harmon, "Warner to Sell Digital Signals Online," NY Times, September 24, 2002 at C9.
19. This is exacerbated by the fact that under the bill, a victim must first ask the Attorney General to decide whether her complaint is a valid one.

Mr. COBLE. Thank you, Ms. Sohn.
Mr. Galdston?

STATEMENT OF PHIL GALDSTON, SONGWRITER-PRODUCER

Mr. GALDSTON. Mr. Chairman, Mr. Berman, Members of the Subcommittee, I appreciate this opportunity to share my thoughts on musical intellectual property and threat posed to the creators and owners of it. Just as importantly, I thank you for examining issues crucial not only to songwriters and music publishers but to music lovers around the world.

As my bio states, I am a composer, lyricist, and music publisher. I am not a recording artist. I make a living and support my family by writing songs and submitting them to performers, producers, managers, labels, and anyone else who may help me get them recorded and exposed to the public.

Over the course of my career, I have been fortunate enough to score hits on most major charts. My greatest achievement and my greatest asset is the catalog of over 600 songs I have created in 37 years of writing. I am here today because that asset—my personal property—is under attack and is the subject of outright theft by those who obtain it without my permission and without compensating me.

Please make no mistake: songwriters' livelihoods are seriously and negatively impacted by unauthorized downloading of our work through peer-to-peer networks.

While there is little doubt in my mind that the solution to this crisis is multifaceted, at least part of that solution requires that our elected representatives help us.

To most people, the system compensating songwriters for the use of their work is murky at best. Those who discuss it try to draw analogies between intellectual property and so-called real property. I don't believe that an appropriate analogy exists, and that tells me that what we songwriters create is rather unique.

Real property, of course, is comprised of raw materials that are produced by someone else. You just can't say that about songs. If I don't dream it up from my heart and my head, there will be no song. The question most frequently asked of songwriters is, "Which comes first, the words or the music?" The answer is neither. What comes first is the inspiration, in all its wondrous variety, none of

which, or their final expression, can be defined as "real property." Nonetheless, as you well know, it is property.

To understand how songwriters are affected by unauthorized downloads, it's crucial to realize that except in rather rare circumstances, we do not sell our songs. We license them to record companies and other outlets in return for royalties when and if they sell.

And to keep things simple, I'm going to keep my remarks to sales from mechanism royalties. But the principles apply to both mechanical and performance royalties.

It's not just semantically incorrect to say that people download "record companies' songs"; it is factually incorrect. The record companies don't own the songs. They only own their recordings of those songs. Songwriters, individual creators, own their songs. All the angry talk about the major record labels and their failings unfairly lumps the songwriter in with the labels and ignores this essential fact.

A person who downloads a record of a song of mine without my permission may think that they're punishing what they believe are big, bad record companies or greedy, selfish artists, but they're also punishing me, the person in the creative process who can least afford to be punished, because, if anything, the current licensing system for mechanical royalties already punishes me.

When a license is sold to a record company, I receive nothing. My compensation in that situation depends entirely on the success of the recording. If I am compensated, the already low rate is set by statute. And frequently, labels demand that songwriters accept a three-quarter rate, $.06 per copy sold instead of the current statutory rate of $.08. This is another situation I hope Congress will look into.

While I am sometimes paid less that statutory rate, I am never paid more. In fact, songwriters are the only people I know who are subject to a maximum wage. Although the law guarantees me due compensation for every reproduction of my songs, including digital downloads, I don't receive anything for any of the unauthorized downloads made through P2P networks.

If there are over 3 billion unauthorized downloads per month—well, Mr. Berman has done the math for us—you can see what songwriters are losing. Therefore, while songwriters can see the value of the Internet as a new and potentially vast source of revenue and exposure, while we want music Internet services, including P2Ps to succeed, we must protect our right to be compensated.

It's sad that we songwriters are being punished for our success. The fact that it is difficult to go anywhere in the "civilized world" without constantly hearing songs written by American songwriters is tribute to the immense popularity of our work. Unfortunately, this popularity seems to have led to the misguided notion that because music is in the air, it should or must be free. On the contrary, music is only in the air because my colleagues and I, through inspiration and hard work, have put it there.

All of this is about the basic principles of private property, principles that I have to believe most of those promoting or excusing unauthorized downloads would defend in any other situation. But I am due compensation for the use of my people, and because I'm

not receiving it, no one should download my work without my permission.

So what can Congress do to help copyright owners cope with the damage and the continued threat from our authorized downloads? I think the answer is simple and sensible: Help us help ourselves.

The Berman-Coble bill, as I read it, would provide us with the ability to fight these unauthorized downloads by granting us limited, carefully circumscribed protection from potential liability for engaging in such self-defense. I think this piece of legislation is a good first step and part of the solution.

I believe that you can help us. I hope you are willing to do so. This is about much more than just compensation or permission. This is about the health of music, for who will be drawn to a life creating music if making music cannot provide a livelihood?

This also is about respecting each other's property. My wife and I have taught our children that is wrong to steal, and yet we, all of us, are turning a blind eye to the theft of songs from the people who own them.

Finally, music along with our other powerful cultural expressions is one of this country's leading exports and greatest ambassadors. If we turn our back on those who create it, what will we be saying to our composers and lyricists? To our children? And what will we be saying to the rest of the world?

Thank you.

[The prepared statement of Mr. Galdston follows:]

PREPARED STATEMENT OF PHIL GALDSTON

INTRODUCTION AND BRIEF BIOGRAPHICAL INFORMATION

Mr. Chairman: My name is Phil Galdston, and I am grateful for this opportunity to share some of my thoughts on musical intellectual property and the threat posed to the creators and owners of it. Just as importantly, I thank you for your willingness to examine issues crucial not only to songwriters and music publishers, but to music lovers across the nation and around the world.

As the biographical information I have provided will attest, I am a composer, lyricist, and music publisher. I am not a recording artist (although once upon a time I was one). I am what is known as a pure songwriter—one who makes a living and supports his family by writing songs and submitting them to recording artists, producers, managers, labels, and anyone else who may help me to get them recorded and eventually exposed to the public. For the record, although I do not speak on their behalf, you also should know that I am a long-time writer and publisher member of ASCAP (the American Society of Composers, Authors and Publishers) and a National Trustee and President of the New York Chapter of the National Academy of Recording Arts and Sciences, the group that bestows the GRAMMY© Awards.

Over the course of my career, I have been fortunate enough to score some major hits, and I'm fairly rare in that I have had songs appear on most of the major charts. Among my best known songs are: "Save the Best For Last" and "The Sweetest Days," which are among seven of my compositions recorded by Vanessa Williams; "Fly" and "The Last To Know," which are among five recorded by Celine Dion; "One Voice," which was recorded by Brandy, and was UNICEF's theme song in its 50th anniversary year; "World Without Love," which was a top ten record for the late country star, Eddie Rabbitt; and "It's Not Over (Til It's Over)," which was a top ten pop and rock hit for the rock band, Starship. My songs have appeared on more than 60 million records around the world, and I have been honored with a number of prestigious awards, including a Grammy nomination for Song of the Year and ASCAP's Song of the Year award.

The hits and the awards aside, I am a songwriter and a small-business owner. My greatest achievement, and my greatest asset, is the catalogue of over 600 songs I have amassed in 37 years of writing. I am here today because that asset—my personal property—is under attack and is the subject of outright theft by those who obtain it without my permission and without compensating me. While sharing my

thoughts on that subject, I hope I can shed some light on a few additional, and significantly related ideas, including the basic understanding of music rights as our society defines them and the abundant confusion among the different rights of record labels, recording artists, and songwriters. But please make no mistake about the situation songwriters face: our livelihood is seriously and negatively impacted by unauthorized downloading of our work through peer-to-peer networks.

REAL PROPERTY *VS.* INTELLECTUAL PROPERTY

It would be nice to say that the business community in which we operate has developed a solution to this problem. But that is not the case, and, what's more, it may be extremely difficult to achieve in the short run. While there is little doubt in my mind that the solution to the crisis brought on by unauthorized downloading will be multi-faceted and will require a combination of effective digital rights management technologies, better online access to digital copyrighted material, better enforcement of copyright laws, and new technologies to aid in enforcement, at least part of the solution requires that our elected representatives help protect us.

To most people, the system compensating songwriters for the use of their copyrighted work is murky at best. (The good news, I believe, is that it's no more complicated than the oil depletion allowance or farm supports.) I've noticed that most people who write or speak about music and the rights of those who create it try to draw an analogy between intellectual property and so-called "real property." You know, "downloading a song without the copyright owner's permission is like stealing a bicycle," and the like. After many attempts on my own and with colleagues, I've concluded that an appropriate analogy probably does not exist. That tells me that what we create is rather unique.

Real property is comprised of raw materials that are produced by someone else. You just can't say that about songs. If I don't dream it up from my heart and my head, the song will not exist. The question most frequently asked of songwriters is "which comes first, the words or the music?" The answer is neither. What comes first is the inspiration, in all its wondrous variety of forms, none of which, or their final expression can be defined as "real property." It is property, nonetheless.

RIGHTS TO A SONG *VS.* RIGHTS TO THE RECORDING OF A SONG

To understand the position in which unauthorized downloading places songwriters, it is crucial to realize that, except in rather rare circumstances, we do not sell our songs. We license them to record companies, and other outlets, in return for royalties when and if they sell or are played in broadcast media. For the purposes of this statement, I am going to focus exclusively on the sales—or mechanical—royalty part of our revenue.

There is a given in the music community: "It all starts with the song." That is not only true of a great record or live performance, it's true of the rights that flow from a song's creation. And those underlying rights are separate and distinct from the rights attached to a recording of it. It is not just semantically incorrect to say that people download "record companies' songs." Strictly speaking, the record companies only own their recordings of those songs, not the songs themselves.

The significance of this is that all the angry talk about the major record companies, and their failings (you know, "Why should I pay $18.00 for a CD with only one good song on it?" and the like), when applied to the debate about unauthorized downloading ignores this essential fact of ownership. So, a person who downloads a record without authorization may be trying to punish what they believe are big, bad record companies and greedy, selfish artists. But they're punishing songwriters like me, the people in the creative process who can least afford to be punished.

When I license a song to a record company, I receive no fee, no advance, no payment of any kind. I will only receive compensation when, and if, the recording of my song sells. If I am compensated, the rate, which is already quite low, is set by statute. Frequently, as a condition of recording and releasing a song, labels demand that songwriters accept three-quarters of the statutory rate; in other words, six cents per copy sold instead of the current statutory rate of eight cents. (This is another situation I hope Congress will look into). Please note that, while we may be paid less, we are never paid more. And since we're limited to a maximum of eight cents by statute, we can't charge more elsewhere to make up for the loss.

WHAT SONGWRITERS ARE LOSING

Under law, the compensation we do receive is due us from every reproduction of our songs, including digital downloads. However, we do not receive any compensation for unauthorized downloads made through P2P networks, like KaZaA, Morpheus, or Bear Share. Therefore, while songwriters can see the value of the internet

as a new and potentially vast source of revenue and exposure, while we want music internet services, including peer-to-peer services, to succeed, we must demand that we be compensated for the use of our work. That is our legal right.

If, as the most recent studies suggest, there are over three billion unauthorized downloads per month on all known peer-to-peer servers—well, you can do the math and see what songwriters are losing. Moreover, every time someone downloads a song of mine without my permission, I am losing all that follows from it: the ability to support my family, the capital needed to continue to re-invest in my business, and the economic incentive to continue to create.

THE RIGHT TO GRANT OR DENY PERMISSION

In a peer-to-peer download, songwriters are losing something else: the right to grant or deny permission for that type of use. Of course, this is an essential aspect of ownership of any property. But in this case, it's a point illustrative of the complexity of the interlocking benefits of the use of songs.

For example, although a good number of artists write the songs they record, their rights as recording artists and any artists royalties they may receive from the success of their recordings are entirely separate and distinct from those they enjoy as songwriters. By extension, my rights as a songwriter and any financial gain I may derive from the success of a recording made of it are distinct and separate from those of the artists who records my songs.

There are artists, labels, and artist-songwriters who may very well benefit from permitting audience members to download their work for free. Unlike pure songwriters, artists and labels have alternate sources of income and long-range goals to promote. Celine Dion or Brandy or Beyoncé Knowles may profit more from the sales of concert tickets or t-shirts than they lose from a free download promoting their merchandise. The artist and label may decide that it is more profitable to offer a free download in return for, say, an audience member's e-mail address. That trade provides them with an opportunity to market other products and services. Simply put, that is their choice; it should not be imposed on me. (By the way, I haven't seen a lot of "PHIL GALDSTON, PURE SONGWRITER" t-shirts for sale.)

SONGWRITERS ARE BEING PUNISHED FOR OUR SUCCESS

It is sad to me that, as a group, we songwriters are being punished for our success. The fact that it is difficult to go anywhere in "the civilized world" without constantly hearing songs—the vast majority of them written by American songwriters—is tribute to the immense popularity of our work. Be it a store, a mall, a movie theater, a living room with a TV on, a dorm room with a computer, a restaurant with a radio playing, or even the much-maligned dentist's office or elevator, the soundtrack to our lives is a stream of songs. And I imagine that, for many, this ubiquity, born of popularity, is the source of the misguided idea that, because music is in the air, it should or must be free.

On the contrary, music is only in the air because my colleagues and I, through inspiration, hard work, and perseverance, have put it there. We are due our just compensation for its use, including via download. Just as importantly, as individual creators, we are entitled to decide when and how it may be downloaded. All of this is about the basic principles of private property—principles that I have to believe most of those promoting or excusing or defending unauthorized peer-to-peer downloads would defend in any other situation.

HOW CONGRESS CAN HELP

What can Congress do to help copyright owners coping with the damage and the continued threat from unauthorized downloads? Unless you're going to set up a "copyright police" to investigate and prosecute this wholesale theft, we're going to have to ask you to help us help ourselves. I wish I could see another way around this, but I can't.

The unique problem we songwriters face when our work is pirated is that, unlike the owners of real property, not only can't our property be returned to us, its return would not compensate us. It is the unauthorized use in the form of a download of our songs for which we can never be compensated. So we must find a way to stop the unauthorized downloads.

We're probably most similar to the owners of satellites and cable systems, who face no liability when they use electronic countermeasures to stop the pirating of their signals and programming. However, at this point, due to the wide range of many anti-hacking laws, our legal ability to prevent the theft of our property through peer-to-peer systems is inhibited by a high degree of liability. The Berman Bill, as I read it, would provide us with the ability to stop these unauthorized

downloads by granting us limited, carefully circumscribed protection from potential liability for engaging in such self-help. In my opinion, this piece of legislation—even understanding that it may be possible to improve it—is a good first step.

I know that you can help us. I hope you are willing to do so. In the end, this is not solely about just compensation or permission; this is about the health of music. For, who will be drawn to a life creating music, if making music cannot provide a livelihood? And very importantly, this also is about respecting each other's property. We teach our children that it is wrong to steal. Such unethical or immoral behavior, we instruct them, is never acceptable. And yet, we currently turn a blind eye to the theft of songs from the people who own them.

Finally, music, along with our other powerful cultural expressions, is one of this country's leading exports. It is also one of our greatest cultural and, some would say, political ambassadors. If we turn our back on those who create it, what will we be saying to our composers and lyricists? What will we be saying to our children? What will we be saying to the rest of the world?

Thank you.

Mr. COBLE. Thank you, Mr. Galdston.

Mr. Saaf, you're recognized for 7 minutes.

STATEMENT OF RANDY SAAF, CHIEF EXECUTIVE OFFICER, MEDIADEFENDER

Mr. SAAF. Thank you.

I'd like to start off by thanking Mr. Berman for having the foresight to bring a bill like this to the forefront.

Mr. COBLE. Mr. Saaf, if you would, pull that mike a little closer to you. Thank you.

Mr. SAAF. I want to start off by saying, I am not a lawyer, I have read the bill, and I do not claim to understand all the points of the bill or the law it's affecting.

I'm here as a technologist.

I am the president and CEO of MediaDefender. MediaDefender is the largest developer and seller of the peer-to-peer anti-piracy software this bill is addressing.

I want to make the point of how noninvasive MediaDefender's technologies are, in my testimony. We have been selling our technology for over 2 years. Very little reaction has been seen because of how benign our technology is.

MediaDefender is not trying to quash the advancement of peer-to-peer networking. On the contrary, MediaDefender is a big fan of peer-to-peer networking. We believe it's one of the biggest advancements in the Internet since the Web page and has countless applications. However, MediaDefender is also a fan of copyright law. We don't feel these two positions are in opposition to each other.

Piracy is currently the primary use of peer-to-peer networking. We have consistently seen through our hundreds of reports that we generated that 30 days after the release of a popular piece of copyrighted material, approximately 15 percent of the network will have download that piece of copyrighted material.

With over 50 million regular users of peer-to-peer networking, that calculates to just over 7.5 million illegal downloaders per copyrighted piece of material.

The top-selling album this year, in its first months, sold just over 4 million copies. I think that gives a good scope of the magnitude of the problem.

MediaDefender's technology provides a pleasant medium where peer-to-peer technology and copyright law can live together. There are some technology problems that can only be solved with tech-

nology. The virus industry can only be solved with the anti-virus industry's software. MediaDefender's technology is the only way to stop decentralized peer-to-peer piracy.

The classic example of a decentralized peer-to-peer network is the Gnutella network. It was created as a reaction to the Napster lawsuit as an indestructible peer-to-peer system.

Napster was centralized. There was somebody to regulate. Obviously, it got shut down for copyright infringement.

Gnutella, on the flip side, is completely decentralized. There is nobody to sue and nobody to regulate. It's a free-floating technology on the Internet.

MediaDefender's technology is the only way to regulate a network like Gnutella. MediaDefender technology only affects networks on a macro scale, meaning we don't really pay attention to the individual users much on the network.

MediaDefender's technology participates in the peer-to-peer network like any of the other 50 million peer-to-peer users. Our aim is to prevent the person seeking the pirated material from finding the pirated material. Data is not collected on individuals. Computers and files are not harmed. There is no excessive drain on bandwidth. And legitimate content is still widely available on these networks.

Some of MediaDefender's technologies are completely lawful and have been spoken about here, such as decoying, spoofing, and they're well-understood.

However, other technologies that could be very effective in the fight against piracy happen to overlap with existing computer use and hacking laws that were never meant to address peer-to-peer networking.

Interdiction is the classic example of one of those technologies. Interdiction is where MediaDefender gets in line and downloads content from a person providing content on a peer-to-peer network.

To the end-user providing the content on the peer-to-peer space, it looks just like somebody else is downloading the content from them. People are putting these files to be available on the public Internet space via these peer-to-peer networks, and MediaDefender is just downloading it from them. If we weren't downloading it from them, somebody else would be.

There is no excessive drain on resources when we're doing this, and it doesn't affect the Internet services such as e-mail, Web browsing, or even the other use of peer-to-peer networking. It acts exactly the same as the peer-to-peer networks act.

It's purely coincidental that some current laws overlap with this particular technology. We don't want a MediaDefender noninvasive technology to be illegal due to hacking laws that were never meant to address peer-to-peer self-help technology.

MediaDefender believes strongly in the privacy of individual users. MediaDefender has been able to stay under the radar for over 2 years because of how noninvasive our technology is.

Right now, copyright owners have three options, as I see it. One, you sue the tens of millions of individual contributory copyright infringers on the peer-to-peer networks. Two, you sue the software developers who create the systems. For a system like Gnutella,

where there are thousands of different software developers, that's very impractical. Or three, you use MediaDefender's technology.

MediaDefender's technology is the only way to proactively prevent the economic harm before it occurs. Even if you sue these people, even if you win these lawsuits, the damage has been done; they can't repay the millions of dollars of economic harm they're causing. MediaDefender's technology is actually able to proactively prevent that harm.

Thank you.

[The prepared statement of Mr. Saaf follows:]

PREPARED STATEMENT OF RANDY SAAF

I want to make clear at the outset that I have read the legislation and I am not a lawyer. I do not pretend to completely understand Congressman Berman's proposed peer-to-peer ("P2P") bill nor the current law it is affecting. I am coming here as a technologist and the primary provider of the anti-piracy technologies this bill is directed toward. MediaDefender has a suite of technologies that are clearly legal and are widely deployed for anti-piracy protection on peer-to-peer networks. MediaDefender also has a group of technologies that could be very effective in combating piracy on peer-to-peer networks but are not widely used because some customers have told us that they feel uncomfortable with current ambiguities in computer hacking laws. These computer hacking laws are beyond my means of understanding, but I know that their intention is not to prevent reasonable, non-invasive anti-piracy technology. My aim is to inform you about MediaDefender and its technology. I want the committee to see the non-invasive nature of MediaDefender's technology so that Congress accepts the peer-to-peer bill to allow reasonable self-help technologies on peer-to-peer networks, while still protecting individuals' civil liberties.

MediaDefender has been selling its P2P anti-piracy technologies for over two years and has gone largely unnoticed. MediaDefender's ability to operate "under the radar" is a result of the company's dedication to providing non-invasive technological solutions to the ever growing piracy problem on P2P networks. For the most part, there has been very little opposition to the deployment of our technologies. We have seen very little complaining, and we attribute that to the non-invasiveness of our technology. We all know that there would be a huge outcry if damage was being done to peoples' computers and clearly that is not the case. People might not ever even know this was going on if MediaDefender never came forward. However, MediaDefender feels it is important to come out and speak on this legislation because of how it could dramatically help solve the piracy dilemma on the public Internet.

Most people agree that advances in technology are beneficial to society as a whole. MediaDefender is not trying to quash the progress in computer science that has been gained through the widespread adoption of P2P networking. MediaDefender's stance is that P2P networking is a huge evolution in the Internet and will have countless applications and advantages. MediaDefender is also a fan of copyright law. We do not feel these two stances are in opposition to each other. It is true that the primary use of P2P networking today is piracy. However, there are many companies trying to advance the technology toward more noble goals.

MediaDefender's technology provides a pleasant medium where copyright law and P2P technology can live together. Technology is fostered by technical solutions to P2P anti-piracy. MediaDefender and creators of P2P software are constantly pushing each other to advance our technologies. MediaDefender views this game of cat and mouse as a net gain for all parties because, at the end of the day, we are all left with stronger, more sophisticated technology than when we started. The most analogous situation is the virus/anti-virus industry. When people advance virus technology, companies like Symantec have to develop new technology to solve the new problems. Similarly, when P2P piracy advances occur, MediaDefender has to develop new technology to solve the new problems. Thus, P2P technology is allowed to advance toward the bettering of its legitimate uses, and copyright owners can feel that they are not being driven out of business.

MediaDefender's technologies only affect the networks on a macro-scale and not on a micro-scale. MediaDefender only communicates with the P2P networks on a high level and pays no attention to the individual users. We do not identify, nor target individuals. We do not collect information about individuals. All we see or care about are the numbers. The primary aim of the technology is to prevent the person

who is seeking pirated material from finding pirated material. People's computers are not harmed and files are never altered or deleted. There is no excessive drain on bandwidth resources. Legitimate content is still widely available on the networks because its availability is not affected by the technology. Even piracy advocates have no basis for complaint because a wide assortment of pirated material is still available on the P2P networks. Our technology does not affect the scalability or overall integrity of the P2P networks. As stated earlier, MediaDefender has been selling its technology for two years and that clearly has not hindered the growth of P2P networking. There are nearly twice as many users today as there were in Napster's more popular days. The most popular P2P application receives over 2.5 million downloads a week. I would say that our technology has done very little to discourage the use and adoption of P2P networking as a whole. However, the very specific use of the P2P networks for piracy of our clients' copyrighted materials has been sharply affected. The good news is that P2P networking as a technology can live and thrive even in the presence of piracy control. At the end of the day, this is how it has to be. P2P networking is not going anywhere, and copyright law is not going anywhere. So, they have to learn how to coexist without destroying each other.

The most threatening aspect of P2P networking to the copyright holders is the growing trend of decentralization. All of the most popular P2P networking technologies in the world are either completely or partially decentralized. Decentralization means that there is no central entity to sue or regulate using the law. Even if all the courts agreed to shut a decentralized network down, it could not be done because it is simply a free floating technology protocol on the Internet, similar to FTP or HTTP. The original completely decentralized P2P protocol, Gnutella, continues to be the leader in the decentralized P2P world. Thousands of computer scientists have developed hundreds of programs to hook into this ethereal network that floats on the Internet. Any programmer can very simply code a software client to hook into the network. Nobody owns Gnutella and nobody regulates it. However, the clear and primary use of the network is for the downloading of copyrighted material. This intuitive conclusion has been verified by MediaDefender's years of research. Gnutella was born out of a backlash in the online world toward the Napster lawsuit, and it was created to be an unstoppable P2P technology. Any person can see the breadth of pirated material on Gnutella by putting a generic search string, such as a period (“.”), into any Gnutella client. When I typed a period (“.”) and hit search on a Gnutella client this morning, I received over 1000 returns with content ranging from Eminem to Harry Potter. I advise anyone to perform this simple experiment if they still need to convince themselves P2P networks are primarily used for piracy. Copyright law never anticipated a completely decentralized P2P network on the Internet and cannot prevent the piracy. Sometimes you have to use technology to regulate technology because there is no other practical means. Decentralized P2P networking is a case where there is no other solution beyond MediaDefender's anti-piracy technology. MediaDefender feels that it is important that the current laws do not stand in the way of non-invasive anti-piracy technology on the Internet. The concern is always that hacking and computer use laws not intended to address P2P anti-piracy technologies will be misapplied.

Most current computer law focuses on hacking and does not take into account its implication on P2P anti-piracy technology. The concept of a P2P system like Napster is relatively young and was not around when many computer laws were drafted. Nobody could have anticipated that they would have an impact on legitimate anti-piracy companies. MediaDefender sells a variety of clearly lawful technologies such as Decoying. For the most part this technology is widely understood and accepted. Decoying is accomplished by passively acting as a member of the P2P network on the Internet public space and allowing thousands of files to be downloaded from our computers. The primary purpose of Decoying is to create a needle in a haystack situation which makes the pirated content difficult to find. All P2P networks have two basic functionalities: search and file transfer. Decoying only affects the search functionality of a P2P network and does nothing to the file transfer side. The pirated material is still there on the network, but it is harder to find. Decoying is the most clear and intuitive of MediaDefender's technologies. MediaDefender has several other technologies that, like Decoying, are clearly legal but we cannot go into great public detail on them at this time because there are people whose sole purpose is to overcome our anti-piracy technologies. MediaDefender has another group of equally benign technologies that could be more effective in preventing piracy, but they fall into grey areas of the current computer laws. Therefore, customers will not purchase these technologies. It is not the case that these technologies are particularly invasive, but rather, they just coincidentally fall into grey areas of very complicated hacking laws. We don't want MediaDefender's self help technology to be illegal due to hacking laws which were never meant to address P2P anti-piracy. Obvi-

ously, our customers are not going to risk using a technology that falls into a grey area of the law despite how badly they need that technology.

One of technologies that we are told falls into the grey area of the law is Interdiction. I am not going to try to describe how Interdiction falls into the grey area of the law. I have been assured from our customers that this law is unusually complicated, and it is not trivial to try and understand it. I am not a lawyer, I am a technologist. I simply want to describe the technology and why I feel that it is a good example of a non-invasive technology that can provide societal net gain if used. Fist I want to make it clear that MediaDefender agrees that any anti-piracy solution on a P2P network has to be non-invasive. Peoples' computers and files should never be harmed under any circumstance. However, any P2P anti-piracy technology will inevitably involve communication with individuals' computers located on the P2P network. The P2P networks and their participants exist on the Internet public space. Behind the scenes of a P2P network there is a massive array of communications and data transfers. MediaDefender always participates in P2P networks via their protocols and plays by their rules. What I mean by "plays by their rules" is that MediaDefender does not develop technologies to stop the P2P networks outside the scope of what the P2P networks allow. P2P networks allow file uploading, and that is simply what we are doing with Decoying. P2P networks allow file downloading, and that is simply what we are doing with Interdiction.

Interdiction only targets uploaders of pirated material. The way it targets them is to simply download the pirated file. MediaDefender's computers hook up to the person using the P2P protocol being targeted and download the pirated file at a throttled down speed. MediaDefender's computers just try to sit on the other computers' uploading connections as long as possible, using as little bandwidth as possible to prevent others from downloading the pirated content. MediaDefender's computers do not scan the other computers' ports or hook into other computers exploiting known security weaknesses. MediaDefender only communicates with the computer over the P2P protocol which the user has opened up to the public Internet. The owner of the computer feels no additional impact on their computer beyond what the P2P network already applies. It should not make a difference to the user who they are uploading a pirated file to. In fact, most people who upload files on these P2P networks are bystanders who do not even realizing they are serving pirated content. Most of the P2P networks re-share content when it is downloaded. So, when a P2P user downloads a copy of Madonna's new album, they may un-knowingly become a contributory copyright infringer, uploading that file to thousands of other users.

Interdiction works by getting in front of potential downloaders when someone is serving pirated content using a P2P network. When MediaDefender's computer's see someone making a copyrighted file available for upload, our computers simply hook into that computer and download the file. The goal is not to absorb all of that user's bandwidth but block connections to potential downloaders. If the P2P program allows ten connections and MediaDefender fills nine, we are blocking 90% of illegal uploading. The beauty of Interdiction is that it does not affect anything on that computer except the ability to upload pirated files on that particular P2P network. The computer user still has full access to e-mail, web, and other file sharing programs. Interdiction does not even affect a user's ability to download files, even pirated files, on the P2P network while their computer is being Interdicted. An Interdicted computer may still share up illegal files using other file transfer programs other than that particular P2P network being Interdicted. For example, a user may run two different P2P networks, but MediaDefender is only being paid to Interdict one. The second P2P network will not be affected even though the first is being Interdicted. Multiple computers on the same Internet connection will not be affected if one of those computers is being Interdicted. In practice most users of the P2P networks will not even realize their computers are being Interdicted. The purpose of the networks is for transferring files, and that is simply what is happening. The impact to the person's computer is not noticeably different from when the person is running a P2P program not being Interdicted. Legislation like Congressman Berman's peer-to-peer bill helps clarify that non-invasive self-help technologies, such as Interdiction, are a legitimate form of copyright protection.

Technology like MediaDefender's leaves the copyright holder with options. Right now the options copyright holders have are sue the countless number of P2P piracy systems, go after the tens of millions of contributory copyright infringers, or use MediaDefender's technological solutions. Often times MediaDefender's technological solutions are the only way to prevent immediate irreparable economic harm when a highly anticipated piece of copyrighted material is leaked onto the Internet. Nobody really wants to sue individuals or programmers. The financial loss has already occurred by the time the lawsuit is over, and the infringer is rarely able to correct

the loss to the copyright holder. With tens of millions of P2P users, most of which are in the United States, many people we know and love are downloading pirated material. While downloading pirated material is not legal, it is a much less damaging a crime than making pirated material available for upload. Unfortunately, many of these illegal uploaders are people who are not intending to serve illegal material for download, and do not have the computer savvy to change the settings on the P2P program. Interdiction prevents these people from unintended distribution of copyrighted material. The advocates of MediaDefender's technology do not want to see peoples' computers hurt or privacy invaded. Most want to see technology advance. Elegant solutions to technology problems allow technology to advance without encumbrances of bureaucracy. If legal minds believe the current draft of the legislation leaves too much room for abuse, it should be redrafted. However, the concept should not be abandoned because one thing is certain: P2P technology will continue to improve and illegal downloading of copyrighted material will only get easier.

Mr. COBLE. Thank you, Mr. Saaf.

And thanks to each of the panelists for your contribution.

Now, we impose the 5-minute rule against ourselves as well, so I will start.

Ms. Rosen, it's my understanding that RIAA member companies are already using self-help technologies to prevent digital piracy. Now, some might say, well, if this is the case, is H.R. 5211 really necessary? What do you say to that?

Ms. ROSEN. It's a good question, Mr. Chairman. And I think, as some people have said today, spoofing is perfectly legal. Redirection, as Mr. Boucher I think defines it, or as somebody's testimony defines it, is perfectly legal.

I think the issue is, what do you do about that? What do you about the fact that for every measure you come up with, there's a countermeasure?

I think there's something that Ms. Sohn's testimony doesn't deal with, and that the press just keeps getting wrong on this bill. I'm all for additional cautions being written into the bill, you know, against whatever bad things people think exist. But the absolute fact seems to be that anybody today can go on to one of these networks who is not a copyright owner—I feel like I have to repeat this for the press—anyone today who is not a copyright owner could go on to one of these networks and do everything that Ms. Sohn and Mr. Boucher and Ms. Lofgren said they're worried copyright owners are doing and be subject to less liability than the copyright owners would be if this bill were passed, because this bill actually creates additional liabilities for the copyright owner if they make a mistake.

So anyone could do any of that today and be subject to less liability legally than the copyright owner would be if this bill were passed. That seems to me a lot of protection.

But I'm all for anybody coming forward and putting in whatever additional protections might be necessary for whatever bogeymen people are afraid of in this area. But I think the rhetoric around this issue has just gotten way beyond the facts.

Mr. COBLE. Well, I agree, Ms. Rosen. That's why I mentioned earlier, what I said about the insertion of the fear tactics. Some of the people have very cleverly done that.

Ms. Sohn, let me ask you a question. P2P network designers, I believe, if they so desired, could design their systems to limit copyright infringement. Now, this could avoid much of the need for

countermeasures and many of the efficiency and stability concerns that you've raised. Do you think they should so design it?

Ms. SOHN. Mr. Chairman, the devil's in the details. I mean, yes, copyright owners have rights. And as I said before, I strongly support enforcement of laws to ensure that their rights are enforced and they get remedies.

But the problem is, is depending on you design the network, citizens and consumers have rights as well. They have fair use rights. They have certain, you know, personal rights and personal expectations about the way to use the computer and use the technology.

And so I guess I wouldn't be opposed to it, but I would have to see the details.

Mr. COBLE. I guess the direction from which I come, it seems that they're designed now in such a way that they can circumvent the law. And I don't mean to overly simplify this. You'd think they could design so they could comply with the law; that's my point.

Ms. SOHN. Perhaps they could. I mean, I'm, again—I think peer-to-peer networks—it's in my written testimony—have a lot of great uses.

Mr. COBLE. And I concur with that.

Ms. SOHN. Absolutely. You know, again, I'd have to see how they could design it. Could they design it to stop copyright infringement? Perhaps. Might that also impinge on citizens' rights? That's where the problem arises.

Mr. COBLE. All right, thank you.

Mr. Galdston, in your testimony, you mentioned the often-cited argument that copyright owners should embrace the free file sharing on peer-to-peer networks because it acts or serves as a promotion for music, which in turns generates CD sales.

Elaborate, if you will, how the songwriter is different from the record companies or the recording artists in response to this argument.

Mr. GALDSTON. That's a good question, Mr. Chairman. And I think it's a frequently misunderstood concept that I tried to articulate in my oral statement. Let me go a little farther.

I've had five songs recorded by Celine Dion. I'm very grateful for that. And we are united in our success and in our partnership when my song is sung by her on a record that is released by Sony—not Universal, by the way.

But where we may depart is that Celine Dion has a larger career as a recording artist, and she has a larger business decision to make. She could easily decide that it is worth it to offer a free download of a track or tracks from one of her albums in return, let's say, for securing the e-mail address of somebody who wants to download it, so that she can offer other merchandise. And of course, anybody who is in the music business knows that merchandising is tremendously profitable and successful.

So she may say: I will offer a free download of a track from a forthcoming album, and in return, I'll try to sell a t-shirt.

The problem is, I haven't seen a lot of Phil Galdston t-shirts for sale. [Laughter.]

And that's where our interests diverge, because if she offers for download a recording of one of my songs, I don't get anything where she stands to benefit some other way.

Mr. COBLE. I see that my red light appears. Mr. Saaf, I'll get you on the next round.

The gentleman from California.

Mr. BERMAN. Thank you, Mr. Chairman.

Is the Phil Galdston concert tour a big item?

Mr. GALDSTON. Well, if I might just say, I really appreciated Mr. Wexler's demonstration. It would have been a lot more enjoyable for me if we actually heard the song, though. [Laughter.]

Mr. GOODLATTE. Would the gentleman yield?

Mr. BERMAN. Sure.

Mr. GOODLATTE. That's why I wanted Mr. Wexler to yield to me, to get the music on. [Laughter.]

Mr. BERMAN. Yes. All right, well, I guess it's up to self-help. [Laughter.]

Ms. Sohn, in the statement you gave, you did not make this statement, although you raise the specter of it in your answer to the Chairman's question, you uttered the words "fair use."

I'm curious about fair use on publicly assisted peer-to-peer file-trading systems. Mr. Boucher and Ms. Lofgren and I and others, we've had many discussions about backup copies and how wide the net is in terms of fair use. And there's a lot of interesting discussion about what fair use is.

For the life of me, you surely cannot contend that files put on publicly accessible peer-to-peer systems available to 100 million or more consumers constitutes an act of fair use. But your written statement asserts, and I think you made an oblique reference to it in your response to Mr. Chairman, that a copyrighted work publicly available on a peer-to-peer file-sharing network for downloading without authorization isn't necessarily copyright infringement.

The 9th Circuit Court in Napster—well, let me just preface this by saying, I totally disagree. I think it's clearly an activity which violates a copyright holder's exclusive right to distribution. The Copyright Office agrees. The Ninth Circuit in Napster says Napster users who upload file names to the search index for others to copy violate the plaintiff's distribution rights.

I'd be curious for you to develop how you can contest the notion that making a copyrighted work available for downloading on a public peer-to-peer network doesn't violate the exclusive right of distribution.

Ms. SOHN. Well, just to clarify, I think what I really said in my written testimony was that U.S. copyright law does not include a right to make available, and that is contained in European law but that U.S. law doesn't contain such a right. And in fact, when that has come up, it has been rejected.

So that actually—I didn't discuss the right of distribution. I just talked about the right to make available and that there is no such specific——

Mr. BERMAN. But the reason that the words "making available" don't appear in U.S. law is because Congress in implementing the WIPO treaties, when we passed the legislation implementing them, specifically found that the distribution rights and other rights encompass the idea. They include the idea of making it publicly available. The courts have said that. The Copyright Office has said that.

The fact that two magic words don't appear because we called it something else doesn't mean it's not so.

Ms. SOHN. Right. But it's still not actually part of American law, U.S. law. I mean, yes—look, I'm not defending it. If you're asking me to defend uploading, I'm not going to do it right here.

But that was the only point. It was a very narrow point that I was making in that written testimony.

Mr. BERMAN. All right, well, I mean, so narrow as to—you're not making a case that there's fair use in——

Ms. SOHN. No, absolutely not.

Mr. BERMAN [continuing]. Any of this? All right.

So now we've established—well, do you disagree with the contention Mr. Saaf made, that the primary use of peer-to-peer systems is to trade infringing materials and is, therefore, illegal activity? The primary use, not the worth of the idea, not the brilliance of the technology, not its hope for the future, not the fact that there are many legitimate purposes and positive public benefits from publicly accessible file-trading systems, but that the primary use is to upload and download copyright infringing material? Do you disagree with that, Mr. Saaf's contention?

Ms. SOHN. I guess I don't know—I have not seen enough evidence that that is the case.

Look, I completely agree with you that networks like KaZaA and Morpheus are used a great deal for massive illegal file trading. And we do not support that. But, you know, I can't—I do not know enough to say—to agree with Mr. Saaf particularly that that is the primary reason. And I've seen nothing, actually, in his testimony, other than his statement, to know that that's actually true.

And I do know, as you point out, that there are many, many, many legitimate uses of peer-to-peer technology. It probably will be the killer app to drive broadband, as Ms. Lofgren said. And, again, please don't read my statements to condone any kind of massive peer-to-peer piracy.

Mr. BERMAN. Well, we're making progress. In the next round, we'll continue to try to make more.

Mr. COBLE. I thank the gentleman.

I thank you, Ms. Sohn.

The gentleman from Virginia.

Mr. GOODLATTE. Thank you, Mr. Chairman. This is an excellent hearing. I want to thank all of the witnesses for shedding light on this issue.

Mr. Galdston, I want to especially thank you for putting a human face on this issue. We hear over and over again, it's no big deal to download a song of Celine Dion or Britney Spears because they're mega-millionaires and it has a small impact on them. But for every one of those instances, there is likely to be somebody like you behind them that is making a much more modest living. In fact, most songwriters never write a hit, and many may write one hit. And if they do, that's a very modest living for doing that.

Ms. Rosen, I share your concern about this, too. How many employees are there in the recording industry? Do you know offhand, roughly, all the companies that your organization——

Ms. ROSEN. Well, worldwide, something like a couple hundred thousand.

Mr. GOODLATTE. And most of those people aren't making megamillions, are they?

Ms. ROSEN. And certainly how many employees there are is not relevant to how many people's livelihoods depend on the sale of music.

Mr. GOODLATTE. Absolutely. But most of those people are making modest livings.

Ms. ROSEN. They're independents, right.

Mr. GOODLATTE. And the success of their employment is dependent upon the success of copyright laws protecting the ability to market these products.

And so I share your concern. And I doubt that KaZaA moved to Vanuatu because it's a hub of business activity. They moved there because there are no copyright laws and so that they could act as what I think they are: the home shoplifting network. [Laughter.]

Now, getting to this bill, I see you have a proposal in legislation that would cut those who want to protect copyright loose to do certain things that they're not sure whether they can do right now under current law to protect their copyright. And I see that already the opposition is developing countermeasures.

Do you have countermeasures to their countermeasures? I mean, where are we heading with this?

And I'm going to ask Mr. Saaf in a second what effect on the Internet the deployment of all this technology has. That's one of the concerns that I have that I need some reassurance on.

Ms. ROSEN. Well, Mr. Saaf is certainly going to be more expert than I am in talking about what potential countermeasures there are for these sorts of networks.

But on the policy side, I think it's quite clear that the networks themselves offer the dangers that people are concerned about. You know, as I said before, you can hack, you can plant viruses, you can invade someone's personal computer right now on all of these services because what you do when you sign up is essentially open up your computer to the network. And so the fear of the countermeasures are in some respects no match for the threat that exists today.

So I think we want to simply be in a position on a policy basis and on a legal basis where, as this expert who I saw submitted testimony from the University of Tulsa, one of the few actual experts in information security and file trading said essentially that technological measures are going to have to continue to keep pace with the innovations of the networks themselves. And that was John Hale, I think, from the University of Tulsa.

So we have to be in a position in the marketplace where we can take steps. And so I am all for the kinds of policy prohibitions on what you think people ought not be able to do. But I think the fears of what's possible already exist.

Mr. GOODLATTE. Let me go to Mr. Saaf then.

All of these measures and countermeasures and so on, this escalating warfare that may take place—because we can't reach somebody in Vanuatu to prosecute them as we would like to under the laws, so we're going to deploy these measures—what effect does that have on the operation of the Internet and people's ability to access the legitimate things they want to access and so on?

Mr. SAAF. I mean, ironically, the net gain to the Internet is very positive. What makes the Internet run is software. Software is what drives everything. And when a company like KaZaA, Sharman Networks, comes up with countermeasures to our countermeasures, it becomes this cat-and-mouse game much like the virus/anti-virus industry.

At the end of the day, what everybody is left with is a stronger base of technology than they started with. This isn't the first time that we've seen countermeasures, so to speak, for our technology. This is the first time that maybe there's been a press release on it or that, you know, the press decided to hook into this particular example.

But this is inevitably what is going to happen. This inevitably a cost of business for our company. But in terms of the idea of that harming the Internet in some way, that would be completely off base.

Mr. GOODLATTE. Am I correct that if KaZaA can do that, they could also deploy measures to protect copyrighted materials as opposed to things that are in the public domain?

Mr. SAAF. Yes, absolutely. That's true.

Mr. GOODLATTE. If they were so disposed.

Mr. SAAF. Yes. I mean the idea that—any kind of software product can update itself. Obviously, KaZaA can do massive updates on millions and millions of users. You know, you can make it do anything. You can make it not work. You can make it filter stuff.

Mr. GOODLATTE. They could do it right as well as interfere with people's efforts to protect copyright.

Mr. SAAF. Yes, absolutely.

Mr. COBLE. The gentleman's time has expired.

The other gentleman from Virginia.

Mr. BOUCHER. Thank you very much, Mr. Chairman.

I appreciate the witnesses enlightening us on this interesting set of issues today.

Ms. Rosen, let me begin by asking a couple of questions of you. I am somewhat concerned that the indiscriminate use of robots could result in some Internet users having their service disconnected even though those users are entirely innocent and have not downloaded any unlawful material but simply have entirely lawful material, whether it's in the public domain or whether it's material they've paid for, on their hard drive.

I have a demand letter here, which I think is very interesting. I'd like to describe it to you, and get your reaction to it. It is from something called the Media Force DMCA Enforcement Center. It is directed to UUNet Technologies. It identifies a particular customer of UUNet, with the Internet address. And then it makes a demand that UUNet disable that connection and terminate the Internet service for that particular user.

It then goes on, on the next page, to identify the material which is alleged to be infringing, which apparently the robot revealed in its search of the network. And it identifies the file name as "harry potter book report." Now, apparently the robot was searching for illegally download copies of one of the "Harry Potter" movies and what it revealed was a book report with a file size of 1 kilobyte. Obviously, this was not a downloaded movie.

But the demand was made that the Internet service be terminated for this user. There's another example where the same kind of demand letter was sent to the ISP for a user who had on his drive the "Portrait of Mrs. Harrison" in a jpeg format. Obviously, that was a photograph. And this was revealed in a robot-directed search for illegally downloaded George Harrison songs.

Now, these are innocent users. And yet, the demand has been made of them that their service be terminated. I'm troubled by that. I'm troubled by the indiscriminate use of robots that can create that kind of result.

Now, I don't know exactly what it is that the industry is seeking to have authorized that isn't authorized under current law, but I would have to think that robot searches, intruding as they do into computer space, has something to do with it. So what I would like to ask of you is your response to this set of examples. Are you as concerned about this as I am? And should we as Members of Congress be concerned about what we may be authorizing as an indiscriminate use of robots that could lead to this kind of result, where innocent users are disadvantaged?

Ms. ROSEN. Well, let me say at the outset that we don't use automated notices to ISPs. We actually look at the evidence first and check it before a letter goes out, just to prevent that very thing, misnamed files. So I am certainly not going to defend it. I have no idea who the copyright owner was that made such a mistake.

I do believe, however——

Mr. BOUCHER. Well, I guess in both of these examples, it would be whoever has the copyright to the "Harry Potter" movies and whoever has the copyright to George Harrison songs.

Ms. ROSEN. I understand. And, you know, it's like me asking you why another Congressman believes what they believe. You have no idea. Neither do I.

So I think the issue that you raise, though, is relevant to the DMCA and not this bill. And I think in the DMCA, there are remedies for both that copyright owner and that ISP to deal with that problem.

So I understand the concern, but I think, you know, enforcement is just that. It has tools, and then it has remedies for when there are problems.

Mr. BOUCHER. Let me ask you this, what is it that you're seeking to have authorized that current law doesn't allow you to do? Ms. Sohn and several of us have acknowledged that spoofing, decoys, redirection, various self-help mechanisms that we know about and you've discussed are lawful today.

What is not lawful today that you would like to engage in and that the Berman bill would give you the privilege of doing?

Ms. ROSEN. Well, I have to defer to Mr. Saaf on that. I think the issue for us is not so much that there is a technology plan or that we know what the situation is. I think when Mr. Berman approached this idea with us, the notion was that we ought to think differently about enforcement. We ought to think not about technical mandates on machines, or not about other restrictions on providers. We ought to think about how self-help measures can be expanded and used.

Mr. BOUCHER. Well, Ms. Rosen, let me just say, my time has expired. But I want to make one comment.

It just seems to me that in the absence of a clear delineation of the additional self-help measures beyond what the current law allows that you would seek to have authorized by this bill, that we would be better advised to wait until you come forward with a clear statement of what those measures are, and then we could evaluate each one of those and look at the potential harms that might arise from it and make a decision with that particular measure on the table.

That's really all I have. Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman.

The gentleman from Florida.

Mr. KELLER. Thank you, Mr. Chairman.

And, Mr. Galdston, I want to thank you for——

Mr. COBLE. If the gentleman would suspend. Mr. Galdston, I have been advised by my able staff that I have been mispronouncing your surname. I said "Gladston," I think, and I apologize for that.

Mr. GALDSTON. I only wish that it was the first time that it happened to me in my life. [Laughter.]

Mr. COBLE. The gentleman from Florida.

Mr. KELLER. You reminded me that I inadvertently associated Celine Dion with Universal instead of Sony, so I will apologize. I'm going to go to my room, think about what I've done, and listen to that darn "Titanic" song yet another 200 times. [Laughter.]

You didn't write that one, did you?

Mr. GALDSTON. I was just going to say, could you please listen to one of mine? [Laughter.]

Mr. KELLER. Okay.

Ms. Sohn, have you ever personally downloaded a song from Napster, KaZaA, or another similar service?

Ms. SOHN. I have from Napster, yes.

Mr. KELLER. Okay. You mentioned there's been a lack of enforcement against these illegal downloaders, so I'm trying to make that simpler for them to do, with your admission. [Laughter.]

I'm just kidding you. I'm sure yours was legal.

You encouraged the recording industry to bring lawsuits against the individual file traders, but you also say that you don't believe that making available copyrighted files for download on peer-to-peer networks is an infringement of copyright, correct?

Ms. SOHN. What I said—what I said was that U.S. law does not now include a right to make available. It does not now include that. So yes, I guess the answer is yes. But I'm not defending that practice here.

And what I was concerned about—I mean, my organization is generally concerned about the expansion of copyright laws, okay? And to the extent that that right is not currently in the law, we would be concerned that this law would expand the copyright law to include such a right.

Mr. KELLER. Did you also say that service providers shouldn't be expected to work with copyright owners to identify infringing subscribers absent the filing of a lawsuit?

Ms. SOHN. No, I think I said exactly the opposite. What I said was that copyright owners, or at least the content industries, know with some reasonable certainty who the big file infringers are. And all they have to do to get the name of that particular person is to file a John Doe lawsuit and seek a subpoena under Federal Civil Procedure 45.

The problem is if you start just indiscriminately requesting from an ISP a bunch of names of file infringers, you have serious ramifications vis-a-vis the privacy and anonymity of ISP users.

Mr. KELLER. All right.

Ms. Rosen, she says that the recording industry—"she" being Ms. Sohn—that the recording industry has never brought a lawsuit against individual file traders, and if there's no enforcement, and it's essentially your fault. So what's your response to that?

Ms. ROSEN. Well, I take note that the consistent response to the enforcement issue from people who claim to represent consumers or technology interests are to sue people. And you know, if that's all that's left, you know, that's an interesting scenario.

I think the point that Ms. Sohn was raising, though, was relevant to actually a dispute that's going on right now with an ISP named Verizon, just a small, little company. Actually, one company bigger than our entire industry.

In Congress, in the DMCA, there was sort of a bargain that this Committee struck with stakeholders because ISPs wanted to have no liability for copyright infringement and they wanted to not have an affirmative obligation to monitor their networks. And obviously, copyright owners were opposed to that, and you brought us to the table and said, "No, no, no. We're going to give them that exemption from liability, but ISPs will be required to help you find the direct infringers." That was essentially the original point of the DMCA, the original kind of bargain. And now we're in a position where we can't do that because of people claiming some legal technicalities.

And so all we keep being left with is massive suits against individuals, which are quite expensive and obviously quite cumbersome, when, if you were in a situation where you could identify through the subpoena process contemplated in the DMCA who the infringer was directly, you could send them a warning letter.

Mr. KELLER. Why would you spend $200,000 getting a judgment against a 18-year-old kid who can't pay it? Isn't that impractical?

Ms. ROSEN. It may be practical. Certainly, you're not going to recover the judgment. I think the point that Ms. Sohn is making is the, essentially, deterrence factor of lawsuits. But there's also the opportunity for warning through the subpoena process contemplated in the DMCA that you are actually avoiding in this scenario.

Mr. KELLER. Thank you. I'll yield back, Mr. Chairman.

Mr. COBLE. I thank the gentleman.

I noticed earlier Mr. Berman mentioned Work for Hire. I see a familiar face in the audience who did the Lord's work, helping us negotiate those rocks and shoals and reefs.

Cary, good to see you here. This has nothing to do with P2P, but good to have you here.

Well, I hear that bell ringing. Let's recognize Ms. Lofgren for 5 minutes.

And, folks, we'll have a second round as well, if you all want to come back.

Ms. LOFGREN. Thank you, Mr. Chairman.

You know, I'd like to reflect back a little bit on where we are vis-a-vis DMCA. And I've been chatting with Members sitting on both sides of me about how much the world has changed technologically since we did that bill. And I remember the discussion, and I was very much involved in it, relative to notice and take-down. And I know that none of us were thinking beyond Web sites at the time, because peer-to-peer—maybe it was out there, but it was way out there. I mean, we were just talking about Web sites.

And certainly, as the technology has changed, it is complicated and made, in some ways, dysfunctional some of what we in good faith worked to do there back there a few years ago.

So that's neither here no there, except it's something that we may need to revisit in the future to make sure that these things actually work in a way that we had originally intended.

Getting to perhaps unintended issues, I note in the bill itself that there is a provision that allows the deletion of files if the consumer authorizes the deletion of files. And I'm thinking about how that might happen and my—I mean, shrink-wrap—you know, there's a lot of verbiage in shrink-wrap, and I'm wondering if we could imagine a time where inadvertently anybody who buys anything has permitted file deletion because of what are really contracts of adhesion.

Do you have—I mean, have you thought through this, either Ms. Rosen or Ms. Sohn?

Ms. ROSEN. No. I think, on the broader picture, we are currently engaged in what we think are appropriate and, as Mr. Saaf said repeatedly, noninvasive technologies. I can't see foresee any scenario where it would be in our interests to try and go into somebody's computer and delete a file. I think the most anybody is looking for are the ability to do more sophisticated interdictions and spoofing and redirection.

Ms. LOFGREN. So you wouldn't object if that was just taken out, if there was no way to delete a file even with permission?

Ms. ROSEN. I don't care.

Ms. LOFGREN. Ms. Sohn?

Ms. SOHN. Well, my concern, again, is that we may accept that the recording industry and the motion picture industry have the means to use more benign self-help. My concern is that this bill permits every copyright holder that right to use self-help.

Probably almost everyone one of us in this room is a copyright holder. And not everybody has the means to afford Mr. Saaf's services. So what you're going to get is a lot of homebrewed technology.

I mean, the way I spin KaZaA matter, the fact that they're starting with their own sort of defense, is that it just makes matters worse. It's escalating a war. I call it the Wild West. You can call it a war, whatever. But you're going to have, you know—and we're not just talking about self-help that exists now. There's going to be future self-help techniques as well, and who knows that they can do.

And this bill opens the door not only to what we know now and not only to limited expensive self-help, to what may come in the future and what may be a lot less costly for copyright owners to use.

Ms. LOFGREN. Yes, Hilary, do you have something to add?

Ms. ROSEN. I was just going to go back to my earlier point, which is, any copyright owner has more liability under this bill than a noncopyright owner for doing any nasty thing——

Ms. LOFGREN. Actually, if I can, I don't think that's correct, because the remedy provided in the bill is one that could never be, in fact, utilized, in my judgment.

But I have very little time, and the bells are ringing.

I wonder if I could just ask, before the next round, Ms. Sohn, you caution in your testimony about denial of service attacks and other things that could essentially impair the functioning of the Net itself. Could you expound on that briefly for us?

Mr. COBLE. Ms. Sohn, if you will, do it quickly because we have to go. We have one 15-minute vote and two 5-minute votes, so if you can move along.

Ms. SOHN. Well, the bill—my problem with what the bill permits and doesn't permit is there's nothing in here that prohibits denial of service attacks. And while Mr. Saaf has guaranteed us again that his technology does not engage in denial of service attacks, we can't be guaranteed because of the breadth of this bill.

And even if a person is guilty, okay, is an infringer, and they get a denial of service attack, that is likely to affect the entire network, including innocent users on that network. That's particularly true when it's a tree-and-branch shared cable-modem service, and it's also true on any ISP network to the extent that the ISP has to divert its attention, find out what's wrong. There's no notice as to who did this or why or when. And there could be other things going on an ISP's network that it must now take its resources away and deal with the self-help mechanism denial of service.

So it affects both indirectly and directly other innocent ISP users. And they don't necessary have to people who are on a P2P network.

Mr. COBLE. I thank the lady.

Folks, you all rest easy, and we will return imminently to resume this.

[Recess.]

Mr. COBLE. We will resume our hearing, folks. I apologize to you all. Sometimes these 15-minute votes extend beyond the time frame. We're going to have a second round, but only the gentlelady from California and I are here.

Mr. Saaf, I was going to get you during the first round. Ms. Sohn raised questions or concerns that interdiction-type technologies might prevent a user from accessing the Internet for any other purpose or that they might burden ISPs or other network users directly or indirectly. Are these concerns justified, in your opinion?

Mr. SAAF. No. Actually, the contrary is true. Interdiction is a participation in the network to download files, like anybody else would be participating in the network and downloading files. The only difference is, when our company does it, it does it a throttle-down download speed, meaning that we're actually freeing up bandwidth resources that would have otherwise gone to the peer-

to-peer client. These people are putting files on the public Internet space for being downloaded, and if we weren't downloading them, I guarantee all their queues would be filled up by potential pirates downloading that material.

Ms. Sohn, to be fair, do you want to respond to that?

Ms. SOHN. At the risk of repeating myself, you know, Mr. Saaf has the state-of-the-art, most expensive technology to do this kind of self-help that there is. And perhaps there are others like him. But my concern, again, is that this bill—and again, I do want to put the focus back on this bill. This bill would allow a lot more than Mr. Saaf's technology and technology that isn't so benign and technology that actually could bring down an ISP's network. And there's nothing in the bill either that prohibits denial of service attacks.

I might feel comfortable if the bill did actually have a prohibition or took out of the safe harbor denial of service attacks. But there's no such language in this bill.

Mr. COBLE. Ms. Rosen, I was going to ask you this during the first round, but time caught up with me. In your testimony, you mentioned and demonstrated the RIAA's efforts to educate the public about copyright infringement. Provide some additional details, if you will, about these efforts and what degree of success you've experienced.

Ms. ROSEN. Well, the first thing I'll elaborate on is that it's not just RIAA. We're doing it in conjunction with a significant number of partners in the music community: ASCAP, BMI, NARAS, the artists' unions and musicians' unions, the Nashville Songwriters Association, the Gospel Music Association.

So there are many, many organizations involved.

We have a series of ads, and I think some educational information for everybody on the Web site, MusicUnited.org. And there will be some ad spots, which will begin this evening on different broadcast outlets.

And actually, I have a tape of that spot, a 30-second spot, if the Committee would be interested in seeing it.

Mr. COBLE. What's the duration?

Ms. ROSEN. Thirty seconds.

Mr. COBLE. Yes, that's fine.

Without objection.

[Videotape presentation.]

Ms. ROSEN. That was—in the outlets that these spots will run, they won't need—the artists won't need to be identified for the fans. But for the rest of us, Missy Elliott, DMX, Shakira, Britney Spears, Nelly, a whole host of diverse artists are involved in this campaign.

Mr. COBLE. Thank you.

Ms. ROSEN. Thank you.

Mr. COBLE. Mr. Berman, Ms. Lofgren has a 12 meeting. Are you equally pressed for time?

Mr. BERMAN. I'm chairing a 12 meeting. [Laughter.]

Ms. LOFGREN. I'm hosting.

Mr. COBLE. Zoe, if you will, move along and we'll get to Howard.

Ms. LOFGREN. I'll just be very quick, and I appreciate Mr. Berman's willingness to let just make a couple of comments.

I would like unanimous consent to submit for the record a statement made at the Aspen Summit symposium on digital rights this August by the CEO of Roxio.

[The information referred to follows:]

PREPARED STATEMENT OF CHRIS GOROG

The record companies and movie studios have come to Washington saying, "the illegal shared file services are destroying our business." "We can't compete with free downloads."

An often-overlooked fact in this debate is—*they haven't even tried.*

An illegal service like Morpheus is indeed the "celestial jukebox". One can access virtually any song in the world, download it and burn it to CD. A very attractive proposition. MusicNet, on the other hand, the service owned by Warner Bros and BMG, doesn't even offer their own complete catalogs... and what they do offer must stay on your PC. I haven't been to too many parties where everybody gathers around the computer to listen to tunes.

The five major record labels are each involved in legal music download services. These companies are part of the largest communications conglomerates in the world and yet, have you seen a single advertisement for the services they own; MusicNet or Pressplay? They could be promoting their services with their movies and television shows, at their retail outlets and theme parks, but instead—nothing. A cynic might conclude that they have absolutely no intention of making these on-line ventures successful.

Why should the Federal Government take seriously the complaints of an industry that has almost limitless capabilities and influences on the consumer—that has done virtually nothing to compete in the on-line world.

Michael Eisner recently went to Capital Hill and had a high profile complaint session, "the movie business will be destroyed, etc., etc." *Where is Disney's on line movie service?* That's right. They don't have one. It's easy to be destroyed if you don't even show up for battle.

The incredible irony in all of this is that every major third party study that I have read recently points to on line distribution as the *savior* of the entertainment industry. Imaging turning your back on an opportunity to rip billions of dollars out of your cost structures and deliver to consumers exactly what they want, instantly, when they want it.

Instead the entertainment companies have burdened lawmakers with poorly thought out schemes like the Digital Millenium Copyright Act which tramples on the consumer's fair use rights and now the Hollings Bill that asks technology companies to become digital policemen.

So what should Government do? I have two suggestions:

1. Tell the record companies and movie studios to come back to Washington after they have actually *tried* to compete. They were just as fearful of television, home video and DVD and those technologies only dramatically added to their businesses. Virtually every industry analyst believes on line distribution will be the same. The entertainment companies must listen to what their consumer is asking for; a fun, easy to use, fairly priced on line service where they can access anything, and burn it to CD and DVD. The entertainment companies and their artists need to stop fighting amongst themselves and—get it done.
2. The Government should do *whatever it can* to help destroy the illegal shared file services. I am convinced the entertainment companies can successfully compete against the illegal services with their vast resources, quality downloads and creative marketing, but, theft of intellectual property cannot be tolerated. It is "IP Terrorism" and extreme measures should be taken to eliminate piracy as much as possible.

Ms. LOFGREN. I think one of the issues that we need to ask about at this hearing, and really after this hearing, because we floated some issues here today, but I think we all know this is a subject that is going to be discussed for some time into the future, and it's an important subject. And I think to that extent, this hearing has served a purpose.

But I think the lack of competition, it doesn't excuse illegal behavior. I don't argue that. But it doesn't confront it and defeat it either. And that is one of the concerns that I have.

It is true that illegal services, as Chris Gorog pointed out, are kind of like the celestial jukebox. But the competing, lawful music—digital music distribution efforts haven't even been advertised. And we've seen an advertisement against piracy, which is fine. I've never seen an advertisement on TV about Pressplay or MusicNet, and I sort of wonder why isn't the lawful alternatives being marketed? And why isn't it user-friendly?

Chris was mentioning the inability to move—burn CDs and move it around on some of these services, and points out that he has not been to too many parties where everybody gathers around the computer to listen to tunes.

I mean, what we need to do is examine the technology efforts that are possible, and there are many; to also encourage—and the Government obviously mandate companies being successful in their endeavor—but to ask for a dialogue about how you intend to be successful in this digital environment, because I really think the incredible irony is that most of the major third party studies that have looked at online distribution see it as the savior of the entertainment business. It is an ability to transmit information while ripping billions of dollars of cost out of the structures that currently exist for entertainment and other—it's not just entertainment. It's other types of content.

And I really think that we, hopefully, as the months go by, we will have an opportunity to engage in dialogue about what content providers, whether it be records, movies, books, or whatever, are going to do to market successfully the digital distribution of their material.

And with that, I would yield back my time to the Chairman and to the Ranking Member, with thanks and apologies for having to leave.

Mr. COBLE. I thank the gentlelady. And we are on a tight time frame. I think Mr. Berman has to Chair a hearing at 12 as well.

Mr. Wexler, with your permission, I'll recognize Howard first.

Mr. Berman?

Mr. BERMAN. Thank you very much, Mr. Chairman. And I do apologize. I have to leave before the end of this hearing. But Mr. French and your staff and other Members will be here.

Listening to Ms. Lofgren's suggestion, I was wondering if you could perhaps promote some of these online music services with ads on Gnutella and Morpheus and KaZaA. [Laughter.]

Targeted advertising.

But by and large, I tend to think free is even better than cheap for lots of people. [Laughter.]

Ms. Sohn, I gather, from the combination of your testimony, your written testimony, you answers to me, and your answers to, I think it was Mr. Goodlatte, that you think the distribution of copyrighted works on these peer-to-peer systems is wrong but not necessarily illegal because of the making-available issue that you spoke to. And I'm wondering, then, would you support an effort to change the law to make it quite clear that it's illegal, given your premises.

Ms. SOHN. As I said before, I'm not generally in favor of expansion of the copyright law. On the other hand, I guess what I would favor is an educational campaign to let people know that they can in fact segregate copyrighted works on peer-to-peer networks.

One of the assumptions I think that I'm a little bit troubled about that I'm hearing at this hearing is that every unauthorized file sharing, unauthorized trade of copyright works, is necessarily illegal.

Mr. BERMAN. I don't think anybody here has said that. They have said unauthorized trading on publicly accessible peer-to-peer file systems, which are available—you don't trade to a specific person on a peer-to-peer system. You put it up, and 100 million people can have it. They've said that unauthorized trading is illegal and wrong. Do you disagree with that?

Ms. SOHN. Well, let me see if I understood what you said. I do disagree that every unauthorized trade is illegal.

Mr. BERMAN. On peer-to-peer—putting something up for trading, uploading or downloading, on these publicly accessible systems, you don't think that that's illegal?

Ms. SOHN. Again, there's a fair use right, okay? What if there's a clip? Okay, what if——

Mr. BERMAN. What is e-mail? There are a thousand different ways to distribute electronically music within an appropriate fair use right without getting into a big debate about how narrow it is or how wide it is.

I don't know how we get common ground if we can't start with the fundamental assumption that this is something so dramatically different than anything encompassed within fair use notions that we have to focus—if we can't accept that premise, there aren't many more places to go together.

Ms. SOHN. Well, I don't disagree with your premise.

I think what I'm arguing is—and maybe I should just sort of get off the legal, okay—is a very, very narrow point, and that is that not every unauthorized use of a copyrighted work is illegal. There are—maybe——

Mr. BERMAN. We know. This is not a novel point. There is a doctrine of fair use, and it applies, and it's a defense to an infringement case.

Let me move on. Before my time is up, I want to just deal with this. It's illustrative of what we were trying to do with this bill versus what people are saying about the bill, this "Harry Potter" book report.

The bill only provides a safe harbor for technological self-help measures within many constraints done by the copyright owner for his own works, not for any other copyright owner, for his own works.

Just taking the hypothetical that two people have mentioned, or perhaps it's not a hypothetical, perhaps it really happened.

If someone authorized by AOL Time Warner went out to hit the "Harry Potter" book report, I don't believe AOL Time Warner owns the copyright to the "Harry Potter" book report. This would not be within the safe harbor. This bill has no impact whatsoever on that. You have to only do acts within the safe harbor before we can start saying that it allows certain kinds of acts.

So when people raise hypotheticals that have nothing to do with this bill as an attack on this bill, it seems to me that we need to straighten that logic out.

Also, denial of service. The reason people are concerned about denials of service is because they cause damage. If a self-help measure causes damage other than the blocking of an unauthorized file, it's automatically outside the safe harbor and is, therefore, not protected.

So any self-help measures which aren't within the safe harbor are not immunized. And as Ms. Rosen has said, I think now three times, there are remedies now against inappropriate self-help measures that go beyond the law. Those remedies are all available, plus the additional remedy provided for in this bill for conduct that isn't protected by the safe harbor.

I mean, this was not a bill that the record industry or the motion picture industry or some coalition came to me and said, "Would you introduce this bill for us?" This was our effort, hearing different theories—mandating technology, arguments, criminal prosecution—we said, this has a role to play, too. And the staff came up—I'd like to say I thought of it driving to work, but the staff came up with this notion. And we tried to do it in a very balanced basis and to make sure we're only immunizing conduct which is directed at trying to deal with a very serious problem, a problem that many of the critics either never acknowledge or pass over so quickly that it makes me think that they don't really think it's a problem.

And with that, Mr. Chairman, I thank you for your indulgence again. And I'll go off to my meeting. And my guess is, under whoever's leadership, at whatever point, there'll be additional hearings on this issue.

Mr. COBLE. I'm confident this will be revisited.

Thank you, Mr. Berman.

Now, Mr. Issa and Mr. Wexler still have not appeared on the first round, so let me recognize the gentleman from California, and then I'll get to Mr. Wexler next. And then if we have questions for a second round, we'll do that.

Mr. Issa, 5 minutes.

Mr. ISSA. Thank you, Mr. Chairman.

And before I begin questioning, I'd guess I'd like to make an observation, and the observation is it's a sword that cuts two ways. I think up until now our panels have been mostly content providers, mostly people who want to protect their intellectual property, and by definition, mostly support that. I think we have a 3-to-1 appearance here.

And I look forward to seeing people from, if you will, other areas, such as the consumer electronics manufacturers, the software operating system people, and so on, in a panel either later this year or next year, because I think we have to hear from as many sides as possible if we're going to come up with the right guidance for the industry.

However, Ms. Sohn, I'm a little concerned that if you're complaining about this bill with seemingly absolutely no answers that would allow us to deal with a broadly recognized problem, if that continues to be a pattern by those who object to self-help and other remedies, then I'm afraid what's going to end up happening is

we're going to say there's a problem, there's only a solution from one side, and this body undoubtedly, hearing only one side, will adopt that side.

And I want to be fair to you, to say—maybe I've missed it. Maybe you have some positive solutions other than an expensive educational campaign, when so far, from what I can tell, my child and the millions of other children around the country, you can educate them, but if you give them the name of the site, they'll go there faster to get more. I don't believe that educating those who have grown up in a society that thinks that Napster was okay are necessarily going to be effected by us telling them it's wrong.

But, please, I look forward to your comments on that.

Ms. SOHN. Well, I respectfully disagree with you.

Mr. ISSA. I was hoping you would.

Ms. SOHN. I've given four what I think are very construction solutions, which I believe when used together will limit peer-to-peer piracy.

Now, I would venture a guess that there's not one person in this room who believes that you can completely eliminate piracy over peer-to-peer networks or any Internet networks. In fact, the content industries can't eliminate piracy in the real world.

I was told by a content industry lawyer the other day, who works particularly on Internet piracy issues, she said to me, "You know, the people in Los Angeles are telling me forget about this Internet stuff. We've got people in Taiwan," and so——

Mr. ISSA. I hope they said China, not Taiwan, if you don't mind my interjecting the exact location.

Ms. SOHN. Okay. I don't know for sure.

But the larger point is, you can't eliminate it. So the question is, how do you limit it, all right? And I've given four solutions: enforcement of existing laws, employing noninvasive self-help—I am not anti-self-help—promoting competition, and educating the public.

Now, you know, if Ms. Rosen and her colleagues thought that educating the public was so worthless, they wouldn't be undergoing this campaign and having a huge full-page ad in the L.A. Times and the New York Times. And frankly, I commend them for it.

And my organization, which is brand new, is going to seek to do the same on the citizen consumer side. I don't think that those four things taken together are worthless. I think, actually, if they start to percolate, we could have some positive solutions.

My concern is, and this has always been the concern, that in the effort to stop piracy, you harm legitimate uses of computer technology and consumer electronics. That's what I care about. I care about innocent users getting hurt in the crossfire.

And that's my concern with this bill, is that it permits that. Can this bill be saved? I don't know. Again, to use a phrase I said to the Chairman, the devil is in the details.

And something that's much more narrow—I respectfully disagree with Mr. Berman, this is not a narrow bill. There are loopholes in this bill that you could drive trucks through. And the fact of the matter is—and my biggest problem with this bill is that it shifts the burden, okay? It shifts the burden of using these techniques—okay, the content industries have been using them very sparingly

and very cautiously. In fact, when you ask Mr. Saaf who are his clients, he won't tell you, okay?

But by giving them this safe harbor, it shifts the burden on to consumers to start bringing lawsuits. And the fact of the matter is, unless there's a huge amount of damages, consumers are not going to bring lawsuits. They're not going to sue. And that's my concern, is the shifting of the burden.

Mr. ISSA. Okay. And I guess I'll just shift for one quick one.

Mr. Galdston, I guess what I'd ask you is, you know, you've been fairly silent. No one seems to ask you any questions. But you're the person who gets ripped off.

My question to you really is, can you tolerate the status quo? And if not, would you agree that the industries that facilitate it need to do more or we need to act? It's a tough question. [Laughter.]

No, it's not, with all due respect. No, we can't tolerate the status quo or I wouldn't be sitting here. I could be writing a song right now.

In my testimony, I did my best to distinguish the people who I unofficially represent from the business, the record business, through whom we earn a fair amount of our money.

What I hear here that is so disturbing is, I appreciate the refinement of the bill. I even appreciate the phrase "the devil's in the details." Not a bad title, by the way. [Laughter.]

But it seems to me that what this bill, as I understand it—and I'm not a lawyer and I'm, once again, not saying it can't be improved. But what it does that I'm aware of is, first of all, it draws a line that hasn't been drawn before. And it says that, across that line, there's a safe harbor for us as we try to protect or defend ourselves.

At the same time, that safe harbor lowers our liability or clarifies our liability. At that same time, it increases our liability should we make any mistakes, should me make egregious moves.

I appreciate what Ms. Sohn has to say, for example, about not shifting the burden to the consumer. But if we're trying to balance here, tell me who the burden is on. The burden is on us. We are the ones—talk about fair use. I mean, I can roll out the phrases. Fair use? Is it fair the way it's working right now, meaning the download system? Or talk about killer app. Well, who is it threatening to kill? The people in our position.

So I will admit right out in front, not being an attorney, that there's a balancing act here. But as for accepting the status quo, absolutely not. I can't see how it's going to work.

Mr. ISSA. Thank you.

And thank you, Mr. Chairman.

Mr. COBLE. Thank you, Mr. Issa.

The gentleman from Florida, Mr. Wexler?

The gentleman from New York, Mr. Weiner?

Mr. WEINER. Thank you, Mr. Chairman.

I have a question that's part public relations and part technical. Most of the popular shareware programs or the popular peer-to-peer programs allow you to turn off the ability of someone to come in and download from you. And we've got that chart up that talks

about the dangers that are created by allowing people to come in and look around your computer.

It might be a better, frankly, public relations way to approach this thing to scare the bejesus into people to switch off the ability to download off their computer. You know, essentially go and say zero downloads is the amount; I don't know now you do it on the different programs. "Zero uploads that I'll permit from computer."

If you can scare enough people into it, it doesn't matter if the peer-to-peer network keeps working. If people are so frightened about the idea—in fact, deluge the market so that—every time I open up my mailbox, I get a CD-ROM from AOL offering—you know, deluge the marketplace with software to protect yourself from having anyone come in to look at it that automatically activates the turn-off switch on all of your things.

So I have a—by the way, I should tell you that over the break, Mr. Chairman, I was alarmed to learn that all of this talk about "Harry Potter" book reports on the Internet has led to a flurry of sixth graders searching for them. [Laughter.]

Teachers and principals everywhere are chagrined that a book report is available to be shared.

But if you can just, Ms. Rosen, perhaps talk about that as a hand-in-hand effort to your "don't do it because it's immoral." I mean, let's scare folks.

And then I'm going to ask about the technical ability to maybe do that somewhere outside the person's computer. You know what I'm saying? Like somehow figure out a way that you're not going into my hard drive but you're creating some kind of a wall or a filter.

But first on the public relations side, because that's something that we all kind of fear, that someone is coming in and looking around my computer anyway. If we can figure out a way to convince people to just switch it off, so you still have your stuff in there technically but you're not—because I always wondered my more people didn't do that, you know, just say, "All right, I'll take, but I'm not going to give."

Ms. ROSEN. Well, it's funny you should say that. And I should clarify. We've stopped telling people this is immoral because, as politicians know, if you try and convince people of right versus wrong, they have to be starting from the same set of value judgments that you're starting from.

What we discovered more recently than we should have was that people don't really want us to tell them whether it's right or wrong. What they want us to tell them is whether it's legal or not.

And that's what we have started to do.

But as part of this campaign, we have a component which we call "check the box," because everyone of these services, these client softwares that you download into your system, essentially give you the option to not share—"share," in quotation marks—your music or copyrighted files, more importantly, or any of your files, your bank accounts, your personal book reports, anything you want to protect.

Mr. WEINER. Under KaZaA, just so we understand each other, you can have entire programs that are downloaded to you to a CD,

right? You can have entire programs from your computer taken down, not just individual songs.

Ms. ROSEN. Once somebody opens up the hard drive to these networks, they've already violated their own privacy. They've taken that into their own hands.

Mr. WEINER. So you're already looking at doing that on the public relations front.

Ms. ROSEN. So checking the box is an important component. But the bigger picture I think is—and maybe this is a public relations issue as well. We're in the position, as Mr. Issa said, where we get platitudes—and this is no offense to Ms. Sohn, who I think is smart and articulate. But we get platitudes from people about how they're worried about the margins of the abuse. But everybody agrees that, you know, illegal downloading is wrong and the stealing isn't right and copyright owners ought to be able to deal with their infringement.

Everything that we try and do, though, gets fought by this community.

Mr. WEINER. I don't think anyone would fight—I shouldn't say that. I imagine it would be very hard to argue that you should fight an individual's choice to switch it off. So I think that's something you should continue to put—Mr. Saaf, if in the few moments that I have remaining, can you tell me, technically—your statement was a little bit vague and maybe that's because you want to kind of operate without really people knowing how to countervail what you're doing.

But is there a way to do kind of what we do with viruses but kind of one step away from my computer somehow? Is there some way to—I mean, I'm a little creeped out by the idea that Sony or someone else is going to come in and start poking around my computer and say, "I don't like what you're doing here." Is there some way to keep that relationship kind out in the ether a little bit more, to stop these transactions from happening in a way that perhaps can assuage some of our concerns about our piracy?

Mr. SAAF. There's no way to practically do that without individuals actually agreeing to put something on their computer.

If individuals who ran these peer-to-peer programs agreed to run some sort of program on their computer that could turn off the sharing, so to speak, yes, that could be done.

Mr. WEINER. Do you have the ability to write a program that will go into my computer and press the button?

Mr. SAAF. No, not without either putting it on your computer or tricking it onto your computer. There has to be some way to get the program on your program to actually change the settings.

Mr. WEINER. You download a program that's a spoof that includes it a little microprogram that turns off the switch, that's not technologically possible?

Mr. SAAF. It certainly is. It certainly is. I mean, that might be the type of thing—but that's not the type of thing that we engage in. The main reason for that is that we only participate in the peer-to-peer networks according to the rules of the peer-to-peer network. If the peer-to-peer network allows searching, we might do something to try and affect the searching. If the peer-to-peer network allows downloading, we might and try and do something that al-

lows downloading. Actually putting a program on somebody's computer, you know, that might overstep some bounds.

Mr. WEINER. Got it. Thank you.

Mr. COBLE. I thank that gentleman. Are you through Mr. Weiner?

Mr. WEINER. Yes, sir, unless there's a chance for another question.

Mr. COBLE. Thanks, sir.

All right, the gentlelady from Pennsylvania. I say to her, we are still on our first round.

Ms. HART. Wow. Thank you, Mr. Chairman.

And I'd like to echo also the comments of a number of the Members in their opening statements, that your leadership in this Committee, even though I've only been here a brief time, has been fantastic.

Mr. COBLE. Thank you.

Ms. HART. And I expect that you'll still be a leader on these issues.

Mr. COBLE. Thank you.

Ms. HART. A number of universities and colleges are located in the communities that I represent and also around the communities that I represent. I'm from the Pittsburgh area.

And they've expressed concern to me regarding the use of peer-to-peer services in their networks, on their networks. They say that the amount of traffic that these services have slows the university's network and that downloading of these files takes large amounts of space on the university's computers.

Can any of you speak to the impact that these networks have on universities in particular, and any efforts that you may be making to reduce the amount of file sharing on their networks? And I would assume not all of you would have an opinion on that, but those of you who do, I'd welcome it.

Ms. ROSEN. Well, we've been spending a lot of time lately working with university leadership around the country for this very reason, because—in fact, they come to us with this notion of how do you find the balance between allowing their students to use their broadband capacity and their networks for legitimate uses but still prevent the massive amount of disruption that they are experiencing.

And they are experiencing massive disruption because of downloading copyrighted music and movie and videogame files, not because people are overwhelmed with an amount of fair use uses of scientific and technical journals. That's not what they're saying. They're saying they have a problem because of the stealing.

And there are solutions, but they're entirely within their control. They can deal with filtering their own network. They can deal with policies regarding use for their students. And they can deal with technologies that protect their own systems.

And I think more and more we're hearing that universities want to begin to employ those systems because of the costs associated with the burden on the network.

Ms. HART. Your involvement, then, has more or less been that they have asked——

Ms. ROSEN. Yes.

Ms. HART. They've shared with you basically that there's a problem.

Ms. ROSEN. They know their students are violating the law.

Ms. HART. Right.

Ms. ROSEN. They know that their students are at risk legally. They know that there is a secondary liability that extends to them if they don't take steps.

But I think more importantly is—which is why I think they come to us to try and figure out whether we have tools to offer them.

But I think more importantly, they feel it's in their own self-interests because of the points you raised. They're concerned about their own costs and burdens.

Ms. HART. Okay. So you'll continue that cooperation with them as well?

Ms. ROSEN. Yes.

Mr. GALDSTON. Ms. Hart, may I just add something to that?

Ms. HART. Sure.

Mr. GALDSTON. Anecdotally, I'm sure we're all aware of some of these issues at universities, and I don't have anything much to add about that. But I would draw your attention to a statement that I can't quote verbatim, but released by the administration at USC recently to its students as they started the fall term, clearly explaining to them, clearly attempting to draw the line and educate them as to what is legal and what is not legal, what is authorized and what is not authorized.

I think as we try to balance education—and I can tell you, not in this capacity, but I'm very involved with ASCAP, I'm a trustee of the Recording Academy. We're all working on education programs. We participated in the program that Ms. Rosen talked about.

But we're looking for this balance once again, and this is the key. It's great to tell everybody that it's bad. And it's important. It's essential. It's what I said in my statement; it's what I tell my children.

But we have to be looking for other measures to protect ourselves or help us help ourselves.

Ms. HART. Did you say it was USC?

Mr. GALDSTON. Yes.

Ms. HART. Okay, good. We're going to have to follow up with them after a term and find out if they see any difference in the problems that they've had.

Mr. GALDSTON. Yes.

Ms. HART. That will be interesting to see.

Carnegie-Mellon is near me, so we have a lot of students who clearly have a lot of talent. [Laughter.]

It's been a bit of a problem, actually, as a result.

I have a question specifically for Ms. Sohn. I have very little time, but it's regarding the comment in your testimony: peer-to-peer networks, that copyright enforcement measures may seriously tax them by making them less efficient and more unstable. I agree that there's a great potential in this kind of technology, but I've been told about and I've also seen the amount of illegal materials, as we've discussed today, infringing on content, having pornography appear, and other things that shouldn't.

Isn't this content seen as being equally taxing on the legitimate potential of these networks? Do you see that as a problem? And how is this activity, the legal activity especially, contribute to the efficiency and stability of this peer-to-peer technology? And isn't it possible that effectively deployed countermeasures in the long run might help to cleanse these networks of the illegal activity and actually facilitate a positive and legitimate use of that technology?

Ms. SOHN. I agree with your initial assessment. I mean, you know, the fact that there is a great deal of illegal activity and the fact that—is actually harming these networks. I mean, not only from a technological perspective but also really from a public relations perspective.

I mean, one of my concerns is that, you know, the focus is so closely on abuse here, that sometimes, you know, the good uses of these networks are not seen.

The problem with engaging in self-help, particularly of the kind—the invasive kind that I talk about, is that it escalates the bad network activity and invites more. It invites more defense. Again, KaZaA is already starting to do that.

So I don't think, you know, while I think that a lot of illegal activity is not helpful for the network, okay, I think if you continue on with more self-enforcement and anti-self-enforcement and anti-anti-self-enforcement, that will even make the networks less stable and less viable.

Ms. HART. Okay, I see my time is up. Thank you, Mr. Chairman.

Mr. COBLE. Thank you.

Ms. ROSEN. Mr. Chairman, I know Ms. Hart's out of time, but could I just respond to that for—I'll try and be really brief.

Mr. COBLE. Okay. We're going to have a vote in about 20 minutes, but go ahead, Ms. Rosen.

Ms. ROSEN. Well, I just think that the point that was just made by the Congresswoman and Ms. Sohn is so relevant to the problem here, which is that these networks, you know, they're not trying to solve their problem. They're trying to facilitate their use and gain more users by doing measures like that.

So if all of the people who were so worried about maintaining the good uses of these networks and the purity of these networks would put as much pressure on Sharman and KaZaA to clean up their act as they put on us against our efforts, this problem would be dramatically different.

Mr. COBLE. I thank the lady.

Let's try a second round folks. As I said, that bell is going to ring in about 20 minutes.

Mr. Saaf, we have circuitously discussed this question. Let me try to put it to you in maybe clearer terms: How can peer-to-peer piracy prevention technologies ensure that only unauthorized uses of copyright material are prevented without also preventing legitimate file sharing?

Mr. SAAF. Yes, that's a very tricky question. There are certainly many, many identifiers a file has on a peer-to-peer network. That example that was presented by Mr. Boucher I felt was a very peculiar example because, you know, automatically, you're not going to flag things that are text files or flag things that are not MP3s or not movie files. That's just almost silly. I don't really understand

how that example even—that's, I think, maybe a one out a million situation.

There are things from file name identifiers. Oftentimes file name identifiers are a great way to, you know, get through it, because most things labeled "Harry Potter" on the network are, indeed, "Harry Potter."

Obviously, file type identifiers are very important. File size identifiers are very important. But even cutting through all of those, all the peer-to-peer networks have different types of hashing technology that they use within their network to identify files so that they can splice those files together, so that they can do all their magic behind the scenes.

Those same types of things are available to companies like ours to identify files to extreme certainty.

Mr. COBLE. I thank you.

The gentleman from Virginia.

Mr. GOODLATTE. Thank you, Mr. Chairman.

First, let me assure the gentleman from New York that there is software on the Internet available to all those teachers to search out the book reports. [Laughter.]

So it's probably not a very copyright——

Mr. WEINER. I've got my money on the sixth graders. [Laughter.]

Mr. GOODLATTE. The University of Virginia has had a big to-do about that.

Let me ask Ms. Rosen and then Ms. Sohn, Congressman Boucher suggested a modification to this legislation that I would not agree with, that I would be concerned about, where he said, list the specific things you want to do in the legislation, and then we'll review those and approve it. I think that's a very bad idea because the technology changes so rapidly that you couldn't possibly expect the slow-moving Congress to keep up with those sixth graders or anybody else that is developing technology to enable people to use this.

But what about some parameters that address some of the concerns that have been raised today? Are there some things we could say, in this bill, "Don't do this particular thing"?

Ms. ROSEN. I would certainly support whatever narrowing of the carve-out that people think are appropriate to guard against the sort of attacks that people seem to be so worried about. Although, again, I point out, that can exist today and it shows up.

But I think the problem with going the route that Congressman Boucher says is almost like saying, "Well, for assault laws, we're not going to say you're not allowed to hit somebody. What are statutes are going to say is: You have to kiss. You have to be nice. You should hug."

It doesn't—there just aren't enough things and ways to talk about what you ought to do. What Congress' responsibility, I think, ought to be is to delineate the things that you don't think ought to be allowed.

Mr. GOODLATTE. Right. I agree. I agree.

Ms. Sohn, do you have some specific things that you'd like to see in this bill that, say, we should not do?

Ms. SOHN. Well, there are a lot of parts of this bill that—clearly that are problematic and in my written testimony.

But just to sort address the point of being specific, I guess I don't have as much of a problem with being specific because you can always write into a bill a review, a subsequent review, to, you know, look at new technologies. The Federal Communications Commission does that all the time. They do it, for example, with universal service.

So if you actually list the self-help techniques, it doesn't mean it's frozen there if, you know, include some sort of periodic review.

You know, I'm not opposed to some sort of——

Mr. GOODLATTE. Let me interrupt you on that point and say, instead of having to update this every time technology changes, what if, initially anyway, until we found out whether some of the concerns expressed were correct, what if we had a sunset provision in this bill, so that it was allowed for a year or 2 years or something, and then come back one more time for reauthorization following that sunset? But not to look to try to always come back forever and say, "We're going to list these specific technologies, and we're going to update them and change them," and so on every time we do it.

Ms. SOHN. Well, that's, you know, that's another way to go about it. I mean, a third way to go about it is just to really, you know, narrow the definition, if you can even do it technologically, and I don't know, of some of these self-help techniques. Instead of naming them particularly, you know, talk about the actual functionalities of the technology.

I mean, like I said, my organization, you know, will not support safe harbors for technologies that are invasive. Reasonable, noninvasive, don't lead to denial of service, then, you know, we can start to talk.

Mr. GOODLATTE. Well, if you have any specific things along that line of parameters, please submit them to the Committee.

Ms. Rosen, what do you think about a sunset provision?

Ms. ROSEN. I can't speak for everybody, but I think it's a very interesting idea. It's something—we certainly think this whole thing is an experiment, so——

Mr. GOODLATTE. Let me ask one other question that's related very much to this. I understand the issue in the Recording Industry Association of American case with Verizon, one of the issues is whether a provision in the Digital Millennium Copyright Act that provides and expedited process for ISPs to turn over subscriber information for alleged infringers applies to peer-to-peer files, file sharing.

When Congress passed the DMCA, we intended that provision to provide the copyright owners with quick access to this information, so they can go after the infringers directly and take the ISP out of the middle of the process. If the court finds that the DMCA does not apply in this situation, and I think it should, should the law be updated?

Ms. ROSEN. I can't get away from this issue. [Laughter.]

You know, I think, actually, the Verizon dispute is very relevant to your last question, because what we're sort of faced with is, we've had a great relationship with the ISPs for several years after the DMCA passed. I think even they would say we were careful and thoughtful about the kinds of things we asked them to do.

But what happened when the DMCA was written was that it said—it was technology-specific. So it said, you know—at the time, all the files—nobody had enough capacity on their computers. All the files were always hosted on the ISP's server. It wasn't that that was a deliberate strategic policy decision to write the bill that way. That's just how the technology was working then.

And so that's what the bill says, that when the, you know, the ISP has the responsibility when the file is on its server to give the name of the person who posted the file on their server to the copyright owner. Now that the file's not sitting on their server, but they're still their customer, they're still providing the exact same access, Verizon and others are taking the position, "Well, it's all different now, because that's not what was intended."

But I believe it is what was intended. It's just that the files are technically in these peer-to-peer networks, sitting on an individual's computer instead on the ISP server. But everything else is the same.

So the ISP's logic about privacy doesn't really fly, because they would be—they would give us the name if the file were still hosted the way it was a few years ago. And in fact, they did give us the names then.

So it's very unfortunate, an unfortunate result of statutes being too technologically specific.

Mr. GOODLATTE. Mr. Chairman, I see my time has expired. Thank you very much.

Mr. COBLE. The gentleman's time has expired.

The gentleman from New York.

Mr. WEINER. Thank you.

Ms. Rosen, I just, as we've been speaking about this, been jotting down the things I think consumers are looking for as a way to wean them, and I'm sure you've been spending an enormous amount of time thinking about this as well. I'm just going to go down this list of six or seven items, and if you can just give me a yes or no, do you think the industry has found a way to package it to essentially compete with the things that the——

Ms. ROSEN. I promise you, there's no yes or no on these, but go ahead.

Mr. WEINER. I bet you there is. I bet you there is.

Speed? Is the speed of download that's offered at the sanctioned sites comparable or better than what's being offered on KaZaA's?

Ms. ROSEN. Yes, because speed relies on the person's Internet access.

Mr. WEINER. Right. I understand.

Reliability? When you go to click on something, it's going to be the song that you think it's going to be?

Ms. ROSEN. Yes.

Mr. WEINER. Can you get the old stuff?

Ms. ROSEN. Sometimes.

Mr. WEINER. That's a no.

Ms. ROSEN. Sometimes.

Mr. WEINER. I'm just giving you some working notes on when you go back to the shop, to figure out how far you are, because I happen—you know, I'm doing this because I think that, frankly, at

the end of the day, whatever tools we give you, the marketplace has to be persuaded. And this is what——

Ms. ROSEN. I agree.

Mr. WEINER. You've come to the conclusion as well.

Ms. ROSEN. And I say that frequently.

Mr. WEINER. Right.

Security? You're probably yes, you're much—your probably much further along in security concerns than the other guys are.

Ease of billing? Is it a relatively easy matter when someone goes onto one of these sites? I mean, is billing fairly easy?

Ms. ROSEN. The billing is much easier, but it's not quite as easy on KaZaA. [Laughter.]

Mr. WEINER. I bet.

The ability when you download something to put it onto a CD? Can you do that with your services?

Ms. ROSEN. Often, but they're tiered. You buy certain services and maybe you pay an extra $.99 if you want another track.

Mr. WEINER. Bad idea. Bad idea. Pain in the—you're making—it's a pain in the neck. [Laughter.]

Reasonable price? Like, what does it cost if I wanted to respond to this idea that there's only one good song on a record, what would it run me, if I buy a package of 10 songs or however you do it? Is it about a buck, you said?

Ms. ROSEN. Well, most now are subscription services where, you know, it's anywhere from $10 bucks to $25 bucks a month for all you can listen to, so it depends.

Mr. WEINER. Okay. And do they go puff at a certain point and disappear from your hard drive?

Ms. ROSEN. Depends on what you pay for. See, it actually works like the real world works, which is, depending on what you want, you have choices about your purchasing packages.

Mr. WEINER. Right. But I want to get——

Ms. ROSEN. But the real issue that we haven't gotten to, which I think is the point you're making, is, there's not enough of the legitimate content on all of the sites in all of the various ways consumers want it.

Mr. WEINER. I was leaving that one to the last, the element that one-stop shopping is not anywhere close to be——

Ms. ROSEN. But I think we're quite close.

Mr. WEINER. Okay. Well, let me just tell you, I think that, you know, I happen to agree with the tenet of what Mr. Berman has argued that we need to facilitate this stuff. But there has to be a recognition—and I sense from you that it is, and I've sensed from other folks in the industry that there is—that you're still putting a pretty hasty product out there to compete with something that is not only pretty good but it's really cheap.

So I think that in addition to making the argument that it's illegal, in addition to making the argument that it's immoral, in addition to trying to figure out technological solutions, the real way to slay this beast is the way, frankly, this industry is evolved, and that is that you just come up with a better enough mousetrap. You add content, or whatever it is. And I'm sure you're thinking about this, but I think, still, that should be the focus, making the better product.

And if I can just conclude by finishing up with you, Mr. Saaf, about technology. Virus software that stops viruses from coming in——

Mr. SAAF. Yes.

Mr. WEINER. You install, essentially, something on your hard drive that looks at information that comes in from without and tries to make an assessment whether a known virus is there.

Mr. SAAF. Right.

Mr. WEINER. Okay. From my just brief understanding of this—and you have been remarkably kind of circumspect about it. I mean, I still can't get my hands around what it is you do.

From my understanding of this, it's essentially a virus software program that stops things that are not supposed to go out or in from going in or out. Is there a way to do that at the ISP level?

Mr. SAAF. Well, there certainly is a way. I mean, you know, the difference between virus software and what we're talking about here is that people choose to install virus software on their computer. And this is sort of—I draw the analogy to the virus/anti-virus industry, but it's almost the opposite.

Mr. WEINER. Right.

Mr. SAAF. At the ISP level, there may be. I mean, to be honest, I haven't done a lot of technology research into that.

Mr. WEINER. You know, I'm about ready to ask that you be sworn in. I don't know what the heck it is that you do. [Laughter.]

Mr. SAAF. Well, I would be glad to—I mean, I have two examples, basically, that I came here with, and that's decoying—obviously well-understood, create a needle in a haystack situation. And then the other technology I wanted to lay out as an example was indirection, which interdiction means that you have—you know, that pitcher is the potential uploader, and he has five upload slots on his computer, and MediaDefender tries to fill all five of those upload slots, preventing the potential pirate here from being able to get in line to download the material.

Mr. WEINER. I see. So it's essentially an elaborate decoy program.

Mr. SAAF. Yes. It's using the peer-to-peer network exactly as it's intended to be used. That's why I make the point that, if we weren't downloading it, somebody else would be. And we do so at a throttled down download speed, so we're not being—we're being less aggressive on the person's computer than the peer-to-peer network would be naturally.

Mr. WEINER. Got it. So it's the equivalent of having a moving roadblock, where you essentially slow things down and eventually someone says, "I'm going to get off this service and try another one," and they eventually get frustrated.

Mr. SAAF. And the reason it's important is it's like putting your finger in a whole in a dam. If you don't do something like that, you have this, boom, exponential growth of the pirated material. And even by the time you get that one guy to take it off his computer, 50 guys are sharing it up.

Mr. WEINER. Got it.

My time has expired.

Ms. Sohn, you don't have a problem with that, do you?

Ms. SOHN. Well, one of the things that I do have a problem with is, when he's blocking——

Mr. WEINER. Can you speak into the microphone?

Ms. SOHN. I apologize.

When he's blocking the infringing file, he's also blocking the entire rest of that person's hard drive, okay? There's no such thing as selective——

Mr. WEINER. He's blocking the outgoing veins of the operation.

Ms. SOHN. No, no, no. No, no, no. The incoming.

Mr. WEINER. Incoming, outgoing. Irrespective of that, he's taking existing lanes that are available on these things and essentially filling them up. Isn't that just essentially an elaborate decoy or something like that?

Ms. SOHN. Well, no, my understanding about how decoy and spoofing and the like works is that a downloader has to affirmatively take an action, okay, to get a file, to get an illegal file, and then they get something that's other than that, okay? With what Mr. Saaf does with interdiction, there's actually a third party—I don't like to use this because this it is rhetorical, but it's the best word I can come up with right now—is actually attacking your hard drive.

And from what I understand, and Mr. Saaf and I have a very long discussion on the phone last week, is that you can't just block one file. You've got to block the entire hard drive, and the person can continue to—tell me if I'm wrong; I'm not a technologist—the person can continue to download, but other people can't access their file—their hard drive.

Mr. SAAF. The first thing I would say is that uploader certainly is taking an affirmative action. To say an uploader, somebody who is providing stuff for uploading from them, they are certainly making the decision to run that program on their computer. And like you made the point, they can check that box, if they don't want people uploading. So that have made a decision.

We're also making a decision to download from them, like anybody else would be downloading from them. We're not hindering any of their other uses of the Internet. They can still do their e-mail, Web browsing, all that great stuff. We don't use up a lot of bandwidth. They can even still download pirated material on the peer-to-peer network while we're indicting them.

The only thing that's inhibited is their ability to upload to that peer-to-peer network.

Mr. WEINER. It sounds like hoisting them on their own petard, no?

Ms. ROSEN. Yes.

Ms. SOHN. Well, except——

Ms. ROSEN. Exactly.

Ms. SOHN. Unless the hard drive includes——

Ms. ROSEN. That's what it is.

Ms. SOHN. Unless their hard drive includes noninfringing material.

Mr. WEINER. But the hard drive isn't—it's kind of the vein to the outside world is being clogged, not their hard drive. It's essentially using, you know—anyway.

Thank you, Mr. Chairman.

Mr. COBLE. Thank you, Mr. Weiner.

Folks, let me——

Ms. ROSEN. Mr. Chairman, I'm so sorry to do this, but my lawyers won't let me come home if I don't do this.

Mr. COBLE. All right.

Ms. ROSEN. I misspoke about the Verizon piece. The identification portion of the DMCA, Mr. Goodlatte, doesn't distinguish between where the files are hosts. It's the takedown provision that makes that distinction. And the dispute is over whether the identification provision should be interpreted differently than the takedown provision.

Mr. COBLE. Now your lawyers will permit you entry into the office, Ms. Rosen.

Ms. ROSEN. Thank you.

Mr. COBLE. Folks, let me think aloud for a minute. I want to thank the panelists. I want to thank the very patient people in the audience who have stood with us.

It is my belief that many people who illegally download, who commit piracy, larceny, call it what you will, most of these people I don't believe would go into a department store and steal a towel set or go into a hardware store and steal a saw and a hammer. But am I missing something when I say it still comes under the same heading of larceny? I think I'm not missing it. I think it's larceny.

And, folks, I'm concerned about this. I think this has been a good hearing. I appreciate the interest that you all in the audience have shown.

Without objection, I want to introduce into the record Mr. Conyers' statement, Mr. Hyde's statement, and an article that appeared in yesterday's *Washington Post* entitled, "Burned by CD Burners." It was authored by a person who formerly operated a record store in California. And he wrote in his article, "Competing against rivals, even against huge national chains, is one thing. But no one can compete against free."

[The prepared statement of Mr. Conyers follows:]

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Peer-to-peer networks have numerous uses in education, research, professional development, and entertainment, but many have chosen to exploit their capabilities to pirate copyrighted works. I believe this piracy is one of the biggest threats to the content and technology industries, the two industries that have contributed more to our national economy than just about any other.

The same people who wouldn't even think of taking a candy bar from a grocery store—or a shirt from a department store—think nothing of downloading thousands of movies and songs every day from the Internet. They say that it's so easy to take content from the Internet it must be legal and the copyright owners make too much money anyway. In fact, this type of file sharing is nothing less than "virtual shoplifting."

Those who advocate for free file sharing simply don't understand that the money that they refuse to pay goes to all of those who contribute to the creative process. It threatens the viability of record labels, technology companies, and movie studios, and impacts the livelihoods of their employees, artists, actors, songwriters, other creators, and their families.

And we can guess the impact is serious because, on the music side, sales are down this year 10 percent over last year—and last year's level was the lowest since 1993. I'd like to say that it's interesting that people who support file sharing never make their own movies or music available for free on the Internet. In my mind, there is no question that it is wrong, and numerous court decisions have upheld that answer.

The real question is what should be done about it. There has been a lot of movement this year, including hearings in Congress, bills, and deals within the private industry. For instance, the record labels have started to let consumers stream and burn music off the Internet, and the major movie studios and IBM just announced they are working to allow rentals of digital videos. And the broadcasters reached a deal several months ago with the technology companies on how to protect broadcast content from piracy.

It's important to know what the next step should be and what role Congress should play.

[The prepared statement of Mr. Hyde follows:]

PREPARED STATEMENT OF THE HONORABLE HENRY HYDE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Thank you, Mr. Chairman. It has been asserted in the press recently that the rule of law does not apply on the Internet. That taking a DVD or a CD from a store without paying for it may be illegal and should be prosecuted, but that taking the same movie or music off the Internet without paying for it is lawful and should be tolerated. As illogical as this seems, the assertion has been made over and over again by those who either seek to get something for free, or by those who make products on which free movies and music can be enjoyed.

I disagree with the assertion. Principles and laws must be upheld and enforced regardless of the medium. Theft is theft. To argue that bank robbery is illegal, but use of the Internet to steal the same money electronically is lawful is an absurd proposition. Yet when it comes to intellectual property, the argument is advanced by some academics and industry groups as valid. They argue that the nature of intellectual property vis-a-vis real or personal property justifies the taking. Or that it is "fair use" to take an entire work for nothing more than personal enjoyment even though it was never purchased by the user.

Our nation's copyright laws serve a specific purpose—to protect our creations. It is a simple concept that has spawned the world's most sought after movies, music and software. And I applaud the Department of Justice for recently announcing that it will enforce our intellectual property laws on the Internet just as it would in the physical world.

The concept of peer-to-peer technology, empowering individuals around the world to share information on each other's computers, while creating many of its own security and privacy concerns, holds great potential. So far, however, this great technology has been used primarily to allow individuals to copy movies and music on other people's computers so that purchasing the CD, renting or buying the DVD, or even going to see a movie is unnecessary. And because of the nature of the technology, the piracy occurs at a staggering rate. No creator can survive if this remains unchecked for too long.

Technology should advance, but principles and laws should apply consistently. The public needs to understand that Internet theft is no different than any other, and I app laud you, Mr. Chairman, and Mr. Berman, for holding this hearing to help achieve that purpose.

Thank you.

[*The Washington Post* article follows:]

The Washington Post
washingtonpost.com

The Washington Post

September 24, 2002, Tuesday, Final Edition

SECTION: EDITORIAL; Pg. A21

LENGTH: 741 words

HEADLINE: Burned by CD Burners

BYLINE: Stan Bernstein

BODY:

Back in 1969, I opened a record store in the college town of Isla Vista, a few blocks from the University of California at Santa Barbara. I was just 20 and still a student, and I couldn't think of a better way to earn a living than by bringing music to my friends and neighbors.

More than three decades later, I still can't. But that store is now history. Although it outlasted many competitors, this past February it finally met its match. My Isla Vista store didn't fail because I had suddenly lost the ability to contend with legitimate competitors. I had competed against a dozen stores over the years. It went out of business because its customers found a way to obtain the product we sold without having to pay for it. As the sign I left in the window explained: "Morninglory Music is closed for good in Isla Vista, due to lack of business. (There was no way to compete with free downloadable music and CD burners)."

Most of our customers in Isla Vista were students at UCSB. Like those of college students everywhere, their lives were transformed a few years ago by the advent of online services such as Napster. From their point of view, these services were amazingly simple and convenient -- they provided virtually any album, some even before they were available in stores. And best of all, it was free.

Competing against rivals -- even against huge national chains -- is one thing. But no one can compete against "free."

Yet there was one flaw in the Napster approach. It was illegal. Reproducing copyrighted material without permission is every bit as illegal as shoplifting CDs from a record store. If anything, it's worse, because at least music-store owners can take steps to thwart shoplifters.

Napster was shut down by the courts. But it was quickly replaced by a variety of "peer-to-peer" networks, which actually made the problem more widespread. Sales at my Isla Vista store continued to decline, and by last winter, after sales had fallen approximately 70 percent in two years, I was forced to close the doors.

During the final two years, I had come to think of the Isla Vista Morninglory as a kind of canary in the coal mine -- an early warning of a problem that may seem small but that eventually could affect us all.

I have read recently that about 70 million people illegally distribute upward of 3 billion copyrighted works of music on the Internet each month. I have heard young people boasting about the thousands of pirated songs on their hard drives -- songs they routinely "burn" onto blank CDs for their friends. A generation is growing up with the idea that pirating copyrighted music is the normal way to build a collection.

Let's call illegal "file-sharing" what it really is. The term has the connotation of something benign, even charitable. It's actually "file-stealing-distributing-and-receiving-stolen-property." A bit unwieldy and not so pleasant-sounding, but certainly a more accurate description.

And it's not just music. Digital copies of first-run movies circulate freely, if illegally, on the Internet. So do copies of best-selling books. If people continue to pretend that copyright laws don't exist, I believe we are witnessing the death of "intellectual property" as a viable concept.

I understand that technology is transforming the way information and entertainment are distributed. As record labels and recording artists consider offering direct downloads themselves, they might effectively cut out retailers. But that's their prerogative. They should be able to offer their works as they choose. The choice, however -- and the resulting revenue -- should be theirs to make and receive. With file-sharing and digital burning, it's not.

The same forces that killed my small store now threaten a major segment of our economy -- creative industries such as music, movies and publishing. What future do they have in a world in which books, films and music are simply passed around rather than purchased?

Copyright laws have helped the creators and producers of information and entertainment contribute greatly to this country and its economy. If we want to continue receiving those benefits, it's time for the government to enforce the law.

The writer is president of Morninglory Music in Santa Barbara, Calif. This article was submitted through a trade organization known as the MUSIC Coalition (Music United for a Strong Internet Copyright).

LOAD-DATE: September 24, 2002

Mr. COBLE. Now, folks, I think that's the issue that plagues us today. Hopefully, we will be able to resolve it in due time.

To indicate to you what I said about the scare tactics—I don't want to bore you all with this, but a friend of mine overheard two staffers discussing this legislation in the Rayburn cafeteria weeks ago.

And one said, "Oh, Mr. Berman has introduced this terrible piece of legislation, and Mr. Coble has co-sponsored."

"The sky is falling," my friend thought as he heard these two exchange these ideas. And my friend said he couldn't resist doing this, he said, "Well, why is this such a bad piece of legislation? What's your source? What's your authority?"

This is the answer: "Oh, this fellow follows electronics issues real closely, and he assures me this is bad."

Now, this is the sort of vague misinformation going around this thing. And, folks, I don't suggest to you all today that it's all black or white. Very likely, it's subtle shades of gray, as are most issues with which we deal up here.

But, again, I thank you all for being here. I think it has been a good hearing. This matter is not going to be pronounced dead today. The last rites will not be announced today. It will be revisited.

This concludes the oversight hearing on piracy of intellectual property on peer-to-peer networks. The record will remain open for 1 week. Now, I repeat that: For 1 week the record will remain open, so if anybody wants to weigh in, feel free to do so.

The Subcommittee stands adjourned.

[Whereupon, at 12:45 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE LAMAR SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman, the Internet has revolutionized our lives. News, entertainment, information, and education are accessible at the click of a button. But for as many legitimate opportunities as the Internet presents, it also presents temptations to break the law. This hearing highlights some of those, such as illegal downloads over peer-to-peer networks and other forms of intellectual property theft.

Most people would not shoplift a CD in a retail store, but some have a different attitude about downloading the same copyright protected CD using P2P software on the Internet.

Shoplifting and unauthorized downloading of intellectual property are both illegal. Both represent a direct threat to the livelihoods of U.S. copyright creators, including songwriters, recording artists, musicians, graphic artists, journalists, novelists and software programmers.

I support strong private property rights and believe that copyright owners have legitimate concerns about the theft of their property using P2P software on the web.

Curtailing the theft of intellectual property is not confined to the Internet. For example, software companies use a variety of technologies to make their software inoperable if the licensing terms are violated. Satellite companies use electronic countermeasures to combat the theft of their intellectual property.

H.R. 5211, the Peer to Peer Piracy Prevention Act, seeks to address the illegal use of P2P services on a network. As with the software manufacturer that may imbed a code to disable a software program if it is illegally distributed or copied, so this bill seeks to authorize copyright owners to employ technology-driven strategies to prevent the unauthorized distribution, display, performance, or reproduction of their copyrighted works. The purpose of this bill is to discourage the illegal use of publicly accessible P2P services on the Internet.

Copyright owners have legitimate concerns about the theft of their property. Some advocate that the federal government dictate solutions to combat this kind of piracy on the Internet, but I strongly oppose this approach. The solution lies in the private sector, not with the federal government.

This bill allows copyright owners to protect their own work. While I have some concerns about the details of this bill and how it would be implemented, I support the concept behind it and look forward to working on this issue in the future.

PREPARED STATEMENT OF THE HONORABLE HOWARD L. BERMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman, I want to take a moment to reflect on your tenure as Chairman. For those who are unaware, Chairman Coble's tenure as Chairman of this Subcommittee ends with the 107th Congress.

I have tremendously enjoyed and deeply valued our relationship as Chairman and Ranking Member. You have ably led this Subcommittee through innumerable legislative and political challenges, and done so with characteristic charm, willpower, and an always easygoing demeanor.

Your record of legislative accomplishments as Chairman is great. The Digital Millennium Copyright Act. The American Inventors Protection Act. The Sonny Bono Copyright Term Extension Act. The No Electronic Theft Act. The Satellite Home Viewer Improvement Act. The Anti-Cybersquatting Consumer Protection Act. The

Work Made for Hire and Copyright Correction Act. The Madrid Protocol Implementation Act. And innumerable other, less heralded bills.

The American public owes you a debt of thanks for your dedicated service over the past six years. I owe you a personal debt of thanks for including me as a partner in the leadership of this Subcommittee.

Mr. Chairman, thank you for calling this oversight hearing on P2P piracy. There have been some truly outrageous attacks on the P2P Piracy Prevention Act, and I welcome this opportunity to set the record straight.

When we first introduced the P2P piracy bill, I never expected that anyone would challenge the basic premise of the bill: namely, that copyright owners should be able to use reasonable, limited self-help measures to thwart rampant P2P piracy.

Incredibly, some folks actually challenge that premise. The head of a big trade association claims it's legal to make unauthorized distributions of copyrighted works to 100 million P2P users. P2P software companies claim that, even if illegal, P2P piracy causes no harm. Representatives of the computer industry say that only record companies suffer harm, and they deserve it for charging too much. Others vaguely theorize that copyright owner self-help will threaten security or privacy. And still other piracy profiteers attempt to thwart any solution to P2P piracy, then throw their hands up and say it is an insoluble problem.

Let's start with a basic fact. Unauthorized distribution or downloading of copyrighted works on public P2P networks is illegal. To paraphrase the 9th Circuit in the Napster case: public P2P users "who upload file names to the search index for others to copy violate a copyright holder's distribution rights. P2P users who download files containing copyrighted music violate a copyright holder's reproduction rights." Any attempt to say otherwise is a bald-faced attempt to rewrite well-settled law.

Let's move to another indisputable fact. Massive theft of copyrighted works is the predominant use for public P2P networks today. There are now approximately 3 billion files P2P downloads a month. The vast majority of these downloads contain copies of copyrighted works for which the copyright owners receive no compensation.

Now another fact. P2P piracy doesn't just affect the bogeymen—record companies and movie studios. P2P piracy destroys the livelihoods of everyday people.

What do piracy profiteers have to say to Linn Skinner, a Los Angeles needlework designer whose livelihood has been destroyed by Internet piracy? Or about Steve Boone, a Charlotte small businessman who has watched P2P piracy decimate his karaoke tape company? How do they response to Mike Wood, a struggling Canadian recording artist who believes P2P piracy will derail his recording career before it gets off the ground? What do piracy profiteers say to the vast majority of songwriters who make less than $20,000 per year, and have yet to make one thin dime from the massive P2P piracy of their works?

Songwriters can actually quantify their P2P piracy losses. By statute, a songwriter is both entitled and limited to collecting 8 cents for every "digital phonorecord delivery" of sound recordings containing her songs. Each illegal P2P download of a song robs the songwriter of that 8 cents.

Those eight cents may not seem like much, but multiply 8 cents by the reported 3 billion monthly P2P downloads. It calculates out to $240,000,000 dollars . . . a month. Even 1/10th of that amount represents real money to the 5,000 U.S. songwriters.

Now another fact. If piracy profiteers were truly concerned about security and privacy threats to P2P users, they would address the security and privacy threats posed by the P2P networks themselves. A recent white paper by the University of Tulsa Center for Information Security details how KaZaA, Gnutella, and other popular P2P networks expose P2P users to spyware, trojan horses, system exploits, denial of service attacks, worms, and viruses. A joint paper by HP Labs and the University of Minnesota details how the vast majority of P2P users are exposing personal information, such as credit card numbers, to every other P2P user. In fact, the U.S. Courts, the House, and the Senate all block the use of public P2P networks because of the security concerns they pose.

Do the piracy profiteers talk about these real security and privacy concerns? No. And you know why? Because it is the piracy profiteers who put the spyware on the computers of P2P users so they can surreptitiously collect their personal information and sell it to third parties.

Another fact. P2P companies could design their software to stop piracy, but they don't. Grokster has designed its P2P software to filter out pornography, but has it ever tried to filter out copyright infringements? Napster claimed it couldn't stop piracy, but after the court ordered it to do so, it suddenly found a way to stop most, if not all, piracy on its networks.

Rather than looking for solutions to piracy, P2P companies are designing their systems to be better piracy tools. Both Morpheus and KaZaA have upgraded their software specifically to impair the ability of copyright owners to proliferate decoy files through the networks.

Based on all these facts, what can an objective person conclude other than that many companies plan to profit from piracy, and have no intent or desire to stop it?

I look at these facts and figures, at the faces of copyright owners, and I see a problem in desperate need of a solution. P2P piracy must be cleaned up, and cleaned up now. The question is, How?

My P2P Piracy bill is an important part of the solution. The Peer to Peer Piracy Prevention Act is quite simple in concept. It says that copyright owners should not be liable for thwarting the piracy of their works on P2P networks IF they can do so without causing harm.

You might reasonably wonder why we need to pass legislation giving property owners the right to protect their property against theft. After all, the U.S. Supreme Court has held that "[A]n owner of property, who seeks to take it from one who is unlawfully in possession, has long been recognized to have greater leeway than he would have but for his right to possession. The claim of ownership will even justify a trespass and warrant steps otherwise unlawful."

The problem is that a variety of state and federal statutes may create liability for copyright owners engaging in otherwise justifiable self-help.

This is not fair. Copyright owners should have the same right as other property owners to stop the brazen theft of their property. The P2P Piracy bill simply ensures that the law will no longer discriminate against copyright owners.

Obviously, it is critical that a liability safe harbor be appropriately limited. In drafting the P2P Piracy bill, I tried to ensure that only reasonable self-help technologies would be immunized, that the public would be protected from harm, and that over-reaching or abuses by copyright owners would be severely punished.

The most important limitation in the bill is the narrow breadth of the safe harbor itself. The bill says copyright owners get immunity from liability under any theory, but ONLY for impairing the "unauthorized distribution, display, performance, or reproduction" of their own works on public P2P networks. If the copyright owner's impairing activity has some other effect, like knocking a corporate network offline, the copyright owner remains liable under whatever previous theory was available.

Some claim that the bill is not limited in this way. Their claim appears to be that the bill gives a copyright owner immunity for anything she does, as long as it has the effect of stopping piracy on a P2P network. By their logic, the bill allows a copyright owner to burn down a P2P pirate's house if the arson stops the pirate's illegal file trading. Clearly, the bill says nothing of the sort, and no judge or disinterested party could read it that way.

The bill specifically states that a copyright owner cannot delete or alter ANY file or data on the computer of a file trader. Thus, a copyright owner can't send a virus to a P2P pirate, it can't remove any files on the pirate's computer, and it can't even remove files that include the pirated works.

The safe harbor does not protect a copyright owner whose anti-piracy actions impair the availability of other files or data within the P2P network, except in certain necessary circumstances. Some folks have raised concerns about this provision, and I am thinking about alternative language that could resolve their concerns.

The bill denies protection to a copyright owner if her anti-piracy action causes any economic loss to any person other than the P2P pirate.

The safe harbor is also lost if the anti-piracy action causes more than de minimis loss to the property of the P2P pirate.

Finally, the safe harbor is lost if the copyright owner fails to notify the Attorney General of the anti-piracy technologies she plans to use, or if she fails to identify herself to an inquiring file-trader.

Obviously, these limitations would be meaningless if copyright owners did not have adequate incentive to obey them. The P2P piracy bill provides such incentives by subjecting transgressing copyright owners to MORE liability than they have under current law.

This is a critical point: If a copyright owner falls outside the safe harbor, an aggrieved party could sue the copyright owner for any remedy available under current law, AND for an ADDITIONAL civil remedy created by the P2P piracy bill. The bill also gives the U.S. Attorney General new power to seek an injunction against transgressing copyright owners.

The potential for liability under this wide variety of remedies provides copyright owners with strong incentives to operate within the strict limits of the safe harbor.

I think the P2P piracy bill provides a strong starting point for legislation enabling copyright owners to use reasonable self-help to thwart P2P piracy. However, I don't

claim to have drafted a perfect bill, and I welcome suggestions for improvements. I note, however, that while I will listen carefully to those who wish to solve the P2P piracy problem, I will not be so solicitous of those who wish to profit from it.

Thank you, Mr. Chairman.

PREPARED STATEMENT OF THE HONORABLE RICK BOUCHER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Thank you, Mr. Chairman.

I appreciate the Subcommittee holding a hearing on the matter of music distribution across the Internet, but I'll have to confess a preference for a different focus than that of this hearing.

There is a need for legislative action in this Committee to facilitate the lawful distribution of music across the Internet in a manner that assumes that all owners of copyright are paid. Mr. Cannon and I have introduced a comprehensive measure, the Music Online Competition Act, each of the elements of which if enacted into law would help achieve that goal.

The Copyright Office has also recommended legislation to help achieve that goal.

The recording industry can achieve that goal if it will simply place entire inventories on the Web for permanent portable downloading at a reasonable price.

There is a recent Jupiter Media Matrix study which shows that ⅔ of the public values the availability of a broad inventory of music, the assured quality of the download, and the ability to keep the music permanently and move it from one player to another in the personal environment, as more important considerations than price. These ⅔rds of the public would clearly be willing to pay a reasonable price if these other elements of quality, availability, and portability are present.

In my view the recording industry does not need the legislation which the Subcommittee is examining today. It should put entire inventories on the Web for permanent portable download at a reasonable price. That's the way to compete with the lower quality free peer-to-peer services.

Turning to the bill at hand, I question at the outset what it is the industry wants to do under the provisions of the bill that it cannot do under current law.

Spoofing is allowed now. Decoys are allowed now. Redirection to legitimate websites is allowed now. I hope the witnesses will be very specific about what it is that the industry wants to do by way of self help that it can't do at present. And I have other questions:

- Would any of these intended self help mechanisms harm innocent Internet users by slowing down the speed of a shared network such as a cable modem service?
- Would any of these mechanisms permit the recording industry to intrude into the personal computer space of an Internet user? If so, what are the implications of such intrusions for the privacy rights of individuals?
- If any damage is done to hardware, software or data owned by an Internet user, how would the damaged party know who to proceed against? After all, no notice to him is required under the bill that his space is being invaded or who is doing the invading.
- What assurance will there be that material which is protected under the fair use doctrine will not be blocked or disables by a self help invasion?

What are the implications for the Internet's functionality when the inevitable arms race develops as countermeasures are used to block self help mechanisms? I can imagine that if the recording industry launches what amounts to denial of service attacks against Internet users, that denial of service attacks will then be launched against the industry with broad adverse effects on Internet speed and effectiveness to the disadvantage of Internet users generally.

These are a few of the matters that concern me. I hope these questions will be addressed this morning.

PREPARED STATEMENT OF DAVID P. MCCLURE

Mr. Chairman and Members of the Subcommittee:

My name is David McClure, and I am President of the US Internet Industry Association, the oldest and largest trade association representing Internet commerce, content and connectivity. USIIA was founded in 1994 by leading companies in the

online services industry to represent the interests of individuals and companies that do business on the Internet.

Our diversified membership includes Internet service providers from global and national ISPs to small providers serving remote areas nationwide; Internet backbone companies, telephone companies; hardware and software vendors involved in the technologies of the Internet; electronic commerce sites, and service providers to those sites. Our charter is to promote the growth of electronic commerce, content and connectivity through sound public policy and business support.

FIRST, DO NO HARM

I strongly urge this committee, and this Congress, to take no action at this time on the issue of peer-to-peer file sharing. First and foremost because this issue is neither large enough nor serious enough to warrant the attention of the distinguished members of Congress. And because the Internet and music industries are capable of resolving this issue without the intervention of the federal government.

In this we agree with Hilary Rosen, President of the Recording Industry Association of America when she noted, "Congress cannot keep pace with the marketplace, and none of us should expect them to. The marketplace can handle this. The laws are there." [1]

There is a very real danger that the intervention of this committee and the Congress will serve only to harm the natural evolution and operations of the free marketplace, over-riding the interests of consumers and vendors alike in the pursuit of a balance that the marketplace itself will achieve more rapidly and more effectively if simply left to its own devices.

PIRACY ON THE INTERNET

There is no question that some individuals misuse the Internet, and such Internet services as peer-to-peer file sharing, to trade in stolen intellectual property. No one within the Internet industry condones this activity, and the Code of Practice for our Association states clearly that:

> "Members shall respect the rights of the owners of intellectual properties, including software authors and artists, providing proper diligence and reasonable effort to prevent the infringement of copyrights, patents and other protections." [2]

What is at issue is not whether this Internet piracy exists, but the extent to which it exists and the severity of its impact on the financial well-being of the owners of the intellectual property.

FILE-SHARING STUDIES

There is no credible means of correlating Internet file sharing with the loss of revenues by copyright holders. Any claims to quantify Internet piracy, or the impact of file sharing on the revenues of content companies, are little more than wild guesses.

Sales are declining in the music industry. They are down 6.4 percent for 2001, a decline that continues in this year. Forrester Research estimates that the industry will be a 6 percent decline in sales for 2003 as well. Yet revenues to the film industry, which equally claims to be suffering at the hands of Internet file-sharing, increased by 9.8 percent last year to reach an all-time record.[3] The retail software industry, which also blames losses on Internet piracy, had sales of $105 billion in 2001, up 3% over the previous year. It is expected to see similar growth this year.[4]

What's more, studies on the habits of Internet file-sharers—Jupiter Media Metrix, Webnoize, Forrester Research, Ipsos-Reid Corp., and more recently by the Gartner Group—fail to substantiate the claims of heavy losses for content holders.

Forrester Research found that more than two-thirds of the CDs bought in the US sell to consumers who rarely or never download music files. Ipsos-Reid reported that 81 percent of file sharers buy as many or more CDs as they did before they began downloading music from the Internet. Jupiter Research found that 86 percent of veteran file sharers buy as many or more CDs as they did previously.

---

[1] "A Chat with Hillary Rosen," Brad King, Wired Magazine, http://www.wired.com/news/culture/0,1284,39108,00.html

[2] USIIA Code of Practice, Article VI, as adopted by the USIIA Board of Directors January 5, 1995.

[3] "2001 US Economic Review—Box Office", Motion Picture Association of America, at http://www.mpaa.org/useconomicreview/2001Economic/index.htm

[4] Data provided by market researcher NPD Techworld

One independent study after another shows little or no decline in buying habits among file-sharing consumers. In fact, the evidence gathered by the Gartner Group and released this month presents a different view—that file-sharing is actually driving sales of music products, and that without the influence of the Internet the music industry might be suffering a greater decline in sales than it has today.

THE INTERNET SCAPEGOAT

The Internet and other consumer technologies have always been used as a convenient scapegoat for the music industry. The last time sales of music declined, in 1978, the industry blamed its woes on the cassette tape recorder and launched an aggressive campaign under the slogan "Home taping is killing music." By 1980 it was clear that cassettes had not killed music. Instead, consumers had grown tired of Disco. Once the industry produced music that was more interesting, sales improved.

There is no compelling evidence that the Internet is responsible for the current decline in music sales, any more than cassettes were in 1978. Yet the music industry, through its agents and trade groups, has launched a vicious campaign of propaganda and lawsuits against our industry.

They have sent with hundreds of bogus copyright claims sent to ISPs nationwide. They have put a series of Internet companies out of business, and are now in the courts seeking to summarily close others. They have filed suits against the largest ISPs in the nation, and today are preparing to go to court against Verizon in an effort to expand their "digital rights" against the interests of consumers.

They are demanding that ISPs terminate subscribers' Internet accounts at their whim—without first filing any lawsuit against the consumer—and are demanding that the Department of Justice prosecute consumers who use peer-to-peer networks.

Today they are before this committee in an effort to blame their decline in sales on the Internet. But this is a hollow claim that is not substantiated either by the facts or by reason.

The music industry's financial slump is more likely due to the fact that they have raised the price of CDs by 13% in the past two years, in the middle of a major economic downturn that has impacted overall retail sales and sales of consumer electronic products to a much greater degree than the music industry. The decline in sales is also likely due to the fact that they are suffering from a dearth of new talent. And that the industry has been unwilling or unable to offer any type of digital music distribution model of its own.

The music industry is also suffering because it failed to see a major shift in consumer buying habits. The mass-production, mass-advertising and mass-consumption model that has directed American buying habits since the days of Henry Ford have evolved to a new model in which consumers have things their way—how they want it, when they want it, and where they want it. The popularity of file sharing is at its root a signal to the music industry that it is time to rethink their products, packaging and distribution—or face becoming obsolete.

LEGISLATIVE SOLUTIONS

Mr. Chairman, and members of this committee, the problems faced by the music industry were not caused by the Internet and cannot be resolved by any amount of legislation. They are problems created by the industry itself, and the wounds they are suffering are self-inflicted.

It is our belief that the Internet, and the sharing of files over peer-to-peer networks on the Internet, will ultimately evolve into a powerful new market for content holders. Already, an estimated 40 million Americans are engaged in file sharing, and that number will only increase. These consumers are not unwilling to pay for content. They are unwilling to pay for content they do not want, or content that is packaged in a way that is difficult for them to use.

This is an issue that industry can solve. It does not require new legislation. It does not require new powers of enforcement or interdiction. It requires only that the content community and the Internet community continue their productive dialogue toward building a digital distribution model for their products. These two industries, working in concert, have the necessary expertise, resources and incentive to resolve this issue and should be given the opportunity to do so. Crafting this solution will involve a delicate balancing of interests that may at some point be assisted by appropriate legislation, but needs no such assistance now.

The Congress, and this committee, can best serve the needs of American consumers and of the industries involved by allowing this dialogue and the search for industry resolutions to continue unimpeded.

Thank you.

Attachments:
Slate—"The Music Industry's Self-Inflicted Wounds"
Reuters—"Study Faults Media Focus On Copyright Strategy"
Janis Ian—"The Internet Debalce—An Alternative View"
Janis Ian—"Fallout"

Attachment #1 – Slate

moneybox

Hit Charade

The music industry's self-inflicted wounds.

By Mark Jenkins

Posted Tuesday, August 20, 2002, at 8:19 AM PT

2001 may not be the year the music died, but the pop biz did develop a nagging headache, and it's not going away. The recorded-music industry's first slump in more than two decades continues this year; the number of discs sold is slipping and so is the appeal of last year's stars. Britney Spears' latest album has moved 4 million copies—a big number, but less than half what its predecessor did.

The Recording Industry Association of America, which represents the five major labels that dominate CD retailing, would like to blame much of the slide on Internet music-file swapping. Yet there are many other causes, including the fact that the big five are all units of troubled multinationals—AOL Time Warner, Vivendi Universal, BMG, EMI, and Sony—that are focused on short-term gain and have no particular interest in the music biz. There's also been a recession, of course, and resistance to CD prices that have grown much faster than the inflation rate. Perhaps the most important factor, however, is the major labels' very success in dominating the market, which has squelched musical innovation.

In 2001, U.S. CD sales declined 6.4 percent. Sales have continued downward this year, and a Forrester Research study released last week projects a 6 percent decline in 2003 as well. Yet the report disputes the RIAA's assertion that the now-bankrupt Napster and its successors are responsible for the downturn. More than two-thirds of CDs bought in the United States sell to consumers who rarely or never download music files from the Web, Forrester concludes. Another market research company, Ipsos-Reid, reported in June that 81 percent of music downloaders buy as many or more CDs than they did before they started getting tunes from the Internet.

The RIAA, of course, has studies that say otherwise. But anyone who rewinds to the last major music-biz slump will find some interesting parallels. In 1978, record sales began to fall, and the major labels blamed a larcenous new technology: cassette tapes. The international industry even had an outraged official slogan: "Home taping is killing music." The idea was that music fans—ingrates that they are—would rather pirate songs than pay for them, and that sharing favorite songs was a crime against hard-working musicians (rather than great word-of-mouth advertising). Cassettes were so anathema to the biz that Sex Pistols Svengali Malcolm McLaren could think of no more provocative way to launch his new band, Bow Wow Wow, than with a ode to home taping, "C30, C60, C90, Go!"

By the time Bow Wow Wow bowed in 1980, however, the crisis was almost over. It turned out that home taping had not killed music. Instead, the central problem was the collapsing popularity of dance-pop—lively, sexy, but personality-free music whose appeal was broad but thin. They

called it disco back then, and the name has never recovered from the era's backlash. Although usually termed teen-pop, the music of 'N Sync and Britney Spears is not unlike disco: Both are intellectually underachieving, cookie-cutter styles that have made stars of performers not known primarily for their skills as singers, songwriters, or musicians.

In addition to cassettes, late-'70s industry apologists blamed video games for undercutting record sales. There may have been something to that, and the biz faces even more multimedia rivals today: cable TV, the Internet, and DVDs, as well as much more sophisticated video games. Perhaps more important, younger consumers live in a world where popular music is ubiquitous (and therefore less precious) than in the '60s and '70s, when rock was rationed, semi-subterranean, and generation-specific. Some older music fans may hate hip-hop, nu-metal, or techno, yet in general rock today defines parents as much as (or more than) their kids.

The major labels have snubbed older music fans in recent years, yet over-40s now constitute 44 percent of the CD market, up from 19.6 percent in 1992, according to the RIAA's 2001 annual consumer profile. Unfortunately for the majors, the tastes of graying Beatles and Stones fans have fragmented, making them difficult to reach via mass-marketing. These consumers help support the many smaller labels that market alt-rock, world music, new age, reissues, jazz, folk, bluegrass, post-minimalism, and other niche genres.

Meanwhile, younger fans lose interest quickly and often don't develop strong loyalties. They're less likely to investigate a breakthrough act's previous albums or buy its next one. The genres that appeal to under-25 music fans continue to sell, but individual performers fade quickly.

This is a huge problem for the big labels, who still base their marketing on long-term stars who release multimillion-copy blockbusters. One album that sells 10 million copies is more lucrative than 10 that sell 1 million, because once a CD takes off, the only fixed costs are manufacturing and shipping, which are trivial compared to production and marketing. And long-term careers make each album less of a risk, since the most loyal fans will buy everything an artist releases and profits are high on back catalogs that keep selling.

Yet maintaining superstars is hard and getting harder. They require large advances, high royalty rates, and massive production and marketing money. And they keep demanding such things even when their careers tank (notable recent examples: Michael Jackson and Mariah Carey). The risk that a contemporary superstar's latest album will bomb is high, since attempts to reach the widest possible audience can easily lead to banality and overexposure.

In 1980, when the same sort of listener burnout bedeviled the biz and its superstars, salvation came from an unexpected source: MTV, an upstart cable channel that began broadcasting clips by a new generation of British bands simply because the established U.S. performers weren't yet making video clips. Groups like Culture Club, Duran Duran, and the Clash—whose label didn't even release the original version of its first album in the United States till 2000—broke through to a novelty-starved audience. Suddenly, home taping wasn't an issue anymore.

This is just the sort of shock that the music industry needs—and labors so hard to prevent. Since 1980, the mainstream music industry has only consolidated: Five companies control CD sales,

MTV owns a multi-channel music-TV franchise, and a single company, Clear Channel, dominates both the concert business and Top 40 and rock radio. Ironically, if unsurprisingly, the biz has suffered from its near-monopolistic control. Short-sighted labels and tightly programmed radio have bolstered the success of certain styles and performers but prevented anything fresh from breaking through.

In the past, there were many ways to crack the biz: local radio stations, strong indie labels, regional clubs and promoters. Today, there are only a variety of separate-but-unequal circuits (alt-rock being the biggest) whose performers rarely break into the big time. (Of course, many of them don't want to, and some are major-label refugees with no intention of going back.) In erecting bulwarks around their domains, the major music businesses have left no entrance for the serendipity that kept the pop industry lively (and profitable) for decades. Yet the barbarians at those padlocked gates are the only people who can save the major labels' dwindling empires.

Article URL: http://slate.msn.com/?id=2069732

Attachment #2 – Reuters

REUTERS .COM

KPMG study faults media focus on copyright piracy

Last Updated: September 25, 2002 12:01 AM ET

By Bob Tourtellotte

LOS ANGELES, Sept 25 (Reuters) - Media companies must put less emphasis on protecting digital content and instead find ways to make money from digital music and movies if they hope to beat back copyright pirates who threaten their businesses, according to a study released on Wednesday from KPMG.

The tax, assurance and financial consulting firm said the responsibility for finding new digital business models lies with the boards of directors and not just with mid-level managers. With an estimated $8 billion to $10 billion in lost revenues annually, the issue should be a corporate governance matter.

"What we don't see is a real questioning of business models," said Ashley Steel, a partner in KPMG's Information, Communications and Entertainment practice.

"They complain about the Napsters," she said, referring to the bankrupt music swap site that was found to violate U.S. copyright laws. "But why do the Napsters exist, because the marketplace wants them."

Steel said that if the issue "is not on boardroom table ... then that boardroom has problems."

Ever since the 1990s technology boom fueled the drive to put music, movies, TV shows and books on the Web, the world's major record labels, movie and TV studios and publishers have focused on creating software and hardware that prevents people from illegally copying digital content and re-selling it.

The music industry has been the hardest hit with CD sales dropping dramatically over the past few years as so-called peer-to-peer Web sites like Napster were used prominently by people who would trade, for free, digital files of the songs.

The record labels, too, did not collect royalty payments from the swap sites like they would have from radio stations. The labels launched subscription Web sites in answer to the swap sites, but they have failed to meet expectations.

The same scenario is quickly spreading to the movies, although the distribution of digital video content is hampered by slow Web connections for most home computer users.

Still, the KPMG study that polled some 40 top executives from major players to smaller independent producers and Web firms found the media executives focus on encryption software and other technologies to thwart pirates, instead of looking for ways to beat the pirates to the consumer pocketbook.

The study found that some 81 percent of the executives relied on encryption to prevent piracy, but Steel argued that the pirates will always exist.

"The next stage of encryption just means it will take a hacker a couple of days longer," to crack software

codes and make digital copies of material.

She pointed to the home video industry that as far back as 20 years ago was battling video pirates, but the media firms found ways to profit from video in spite of the pirates.

Steel said that in order to build new business models, the companies' digital content must first be valued properly.

The study found that currently only 43 percent of the companies even make some of their content available in digital form, and fully 57 percent of the executives admitted to failing to have a review process in place to determine types of digital content should be deemed intellectual property.

Major global media companies include AOL Time Warner Inc. AOL.N , The Walt Disney Co. DIS.N , Viacom Inc. VIAb.N , Vivendi Universal EAUG.PA and News Corp. Ltd. NCP.AX and Bertelsmann AG BTGGga.DE .

Attachment #3 – Janis Ian

THE INTERNET DEBACLE - AN ALTERNATIVE VIEW

Originally written for Performing Songwriter Magazine, May 2002

** Shortly after this article was turned in, Michael Greene resigned as president of NARAS.*

"The Internet, and downloading, are here to stay... Anyone who thinks otherwise should prepare themselves to end up on the slagheap of history." *(Janis Ian during a live European radio interview, 9-1-98)*

When I research an article, I normally send 30 or so emails to friends and acquaintances asking for opinions and anecdotes. I usually receive 10-20 in reply. But not so on this subject!

I sent 36 emails requesting opinions and facts on free music downloading from the Net. I stated that I planned to adopt the viewpoint of devil's advocate: free Internet downloads are good for the music industry and its artists.

I've received, to date, over 300 replies, every single one from someone legitimately "in the music business."

What's more interesting than the emails are the phone calls. I don't know anyone at NARAS (home of the Grammy Awards), and I know Hilary Rosen (head of rhe Recording Industry Association of America, or RIAA) only vaguely. Yet within 24 hours of sending my original email, I'd received two messages from Rosen and four from NARAS requesting that I call to "discuss the article."

Huh. Didn't know I was that widely read.

Ms. Rosen, to be fair, stressed that she was only interested in presenting RIAA's side of the issue, and was kind enough to send me a fair amount of statistics and documentation, including a number of focus group studies RIAA had run on the matter.

However, the problem with focus groups is the same problem anthropologists have when studying peoples in the field - the moment the anthropologist's presence is known, everything changes. Hundreds of scientific studies have shown that any experimental group *wants to please the examiner.* For focus groups, this is particularly true. Coffee and donuts are the least of the pay-offs.

The NARAS people were a bit more pushy. They told me downloads were "destroying sales", "ruining the music industry", and "costing *you* money".

Costing *me* money? I don't pretend to be an expert on intellectual property law, but I do know one thing. If a music industry executive claims I should agree with their agenda because it will make me more money, I put my hand on my wallet…and check it after they leave, just to make sure nothing's missing.

Am I suspicious of all this hysteria? You bet. Do I think the issue has been badly handled? Absolutely. Am I concerned about losing friends, opportunities, my 10th Grammy nomination by publishing this article? Yeah. I am. But sometimes things are just *wrong*, and when they're *that* wrong, they have to be addressed.

The premise of all this ballyhoo is that the industry (and its artists) are being harmed by free downloading.

Nonsense. Let's take it from my personal experience. My site (www.janisian.com) gets an average of 75,000 hits a year. Not bad for someone whose last hit record was in 1975. When Napster was running full-tilt, we received about 100 hits a month from people who'd downloaded *Society's Child* or *At Seventeen* for free, then decided they wanted more information. Of those 100 people (and these are only the ones who let us know how they'd found the site), 15 bought CDs. Not huge sales, right? No record company is interested in 180 extra sales a year. But… that translates into $2700, which is a lot of money in my book. And that doesn't include the ones who bought the CDs in stores, or who came to my shows.

Or take author Mercedes Lackey, who occupies entire shelves in stores and libraries. As she said herself: "For the past ten years, my three "Arrows" books, which were published by DAW about 15 years ago, have been generating a nice, steady royalty check per pay-period each. A reasonable amount, for fifteen-year-old books. However... I just got the first half of my DAW royalties...And suddenly, out of nowhere, each Arrows book has paid me three times the normal amount!...And because those books have never been out of print, and have always been promoted along with the rest of the backlist, the only significant change during that pay-period was something that happened over at Baen, one of my other publishers. That was when I had my co-author Eric Flint put the first of my Baen books on the Baen Free Library site. Because I have significantly more books with DAW than with Baen, the increases showed up at DAW first. There's an increase in all of the books on that statement, actually, and what it looks like is what I'd expect to happen if a steady line of people who'd never read my stuff encountered it on the Free Library - a certain percentage of them liked it, and started to work through my backlist, beginning with the earliest books published. The really interesting thing is, of course, that these aren't Baen books, they're DAW---another publisher---so it's 'name loyalty' rather than 'brand loyalty.' I'll tell you what, I'm sold. Free works."

I've found that to be true myself; every time we make a few songs available on my website, sales of all the CDs go up. A lot.

And I don't know about you, but as an artist with an in-print record catalogue that dates back to 1965, I'd be *thrilled* to see sales on my old catalogue rise.

Now, RIAA and NARAS, as well as most of the entrenched music industry, are arguing that free downloads hurt sales. (More than hurt - they're saying it's destroying the industry.)

Alas, the music industry needs no outside help to destroy itself. We're doing a very adequate job of that on our own, thank you.

Here are a few statements from the RIAA's website:

1. "Analysts report that just one of the many peer-to-peer systems in operation is responsible for over 1.8 billion unauthorized downloads per month". (Hilary B. Rosen letter to the Honorable Rick Boucher, Congressman, February 28, 2002)
2. "Sales of blank CD-R discs have…grown nearly 2 ½ times in the last two years…if just half the blank discs sold in 2001 were used to copy music, the number of burned CDs worldwide is about the same as the number of CDs sold at retail." (Hilary B. Rosen letter to the Honorable Rick Boucher, Congressman, February 28, 2002)
3. "Music sales are already suffering from the impact…in the United States, sales decreased by more than 10% in 2001."(Hilary B. Rosen letter to the Honorable Rick Boucher, Congressman, February 28, 2002)
4. "In a recent survey of music consumers, 23%…said they are not buying more music because they are downloading or copying their music for free."(Hilary B. Rosen letter to the Honorable Rick Boucher, Congressman, February 28, 2002)

Let's take these points one by one, but before that, let me remind you of something: the music industry had *exactly* the same response to the advent of reel-to-reel home tape recorders, cassettes, DATs, minidiscs, VHS, BETA, music videos ("Why buy the record when you can tape it?"), MTV, and a host of other technological advances designed to make the consumer's life easier and better. I know because I was there.

The only reason they didn't react that way publicly to the advent of CDs was because *they believed CD's were uncopyable.* I was told this personally by a former head of Sony marketing, when they asked me to license *Between the Lines* in CD format at a reduced royalty rate. ("Because it's a brand new technology.")

1. Who's to say that any of those people would have bought the CD's if the songs weren't available for free? I can't find a single study on this, one where a reputable surveyor such as Gallup actually asks people that question. I think no one's run one because everyone is afraid of the truth - most of the downloads are people who want to try an artist out, or who can't find the music in print.
   And if a percentage of that 1.8 billion is because people are downloading a current hit by Britney or In Sync, who's to say it really hurt their sales? Soft statistics are easily manipulated. How many of those people went out and bought an album that had been over-played at radio for months, just because they downloaded a portion of it?
2. Sales of blank CDs have grown? You bet. I bought a new Vaio in December (ironically enough, made by Sony), and now back up all my files onto CD. I go through 7-15 CD's a week that way, or about 500 a year. Most new PC's come with XP, which makes backing up to CD painless; how many people are doing what I'm doing? Additionally, when I buy a new CD, I make a copy for my car, a copy for upstairs, and a copy for my partner. That's three blank discs per CD. So I alone account for around 750 blank CDs yearly.
3. I'm sure the sales decrease had nothing to do with the economy's decrease, or a steady downward spiral in the music industry, or the garbage being pushed by record companies. Aren't you? There were *32,000 new titles* released in this country in 2001, and that's not including re-issues, DIY's , or smaller labels that don't report to SoundScan. Our "Unreleased" series, which we haven't bothered SoundScanning, sold 6,000+ copies last year. A conservative estimate would place the number of "newly available" CD's per year at 100,000. That's an awful lot of releases for an industry that's being destroyed. And to make matters worse, we hear music everywhere, whether we want to or not; stores, amusement parks, highway rest stops. The original concept of Muzak (to be played in elevators so quietly that its soothing effect would be subliminal) has run amok. Why buy records when you can learn the entire Top 40 just by going shopping for groceries?
4. Which music consumers? College kids who can't afford to buy 10 new CDs a month, but want to hear their favorite groups? When I bought my nephews a new Backstreet Boys CD, I asked why they hadn't downloaded it instead. They patiently explained to their senile aunt that the download wouldn't give them the cool artwork, and more important, the video they could see only on the CD.

Realistically, why do most people download music? *To hear new music, or records that have been deleted and are no longer available for purchase.* Not to avoid paying $5 at the local used CD store, or taping it off the radio, but to hear music they can't find anywhere else. Face it - most people can't afford to spend $15.99 to experiment. That's why listening booths (which labels fought against, too) are such a success.

You can't hear new music on radio these days; I live in Nashville, "Music City USA", and we have exactly one station willing to play a non-top-40 format. On a clear day, I can even tune it in. The situation's not much better in Los Angeles or New York. College stations are sometimes bolder, but their wattage is so low that most of us can't get them.

One other major point: in the hysteria of the moment, everyone is forgetting the main way an artist becomes successful - *exposure.* Without exposure, no one comes to shows, no one buys CDs, no one enables you to earn a living doing what you love. Again, from personal experience: in 37 years as a recording artist, I've created 25+ albums for major labels, and I've *never once* received a royalty check that didn't show I owed *them* money. So I make the bulk of my living from live touring, playing for 80-1500 people a night, doing my own show. I spend hours each week doing press, writing articles, making sure my website tour information is up to date. Why? Because all of that gives me exposure to an audience

that might not come otherwise. So when someone writes and tells me they came to my show because they'd downloaded a song and gotten curious, I am thrilled!

Who gets hurt by free downloads? Save a handful of super-successes like Celine Dion, none of us. We only get helped.

But not to hear Congress tell it. Senator Fritz Hollings, chairman of the Senate Commerce Committee studying this, said "When Congress sits idly by in the face of these [file-sharing] activities, we essentially sanction the Internet as a haven for thievery", then went on to charge "over 10 million people" with stealing. [Steven Levy, Newsweek 3/11/02]. That's what we think of consumers - they're thieves, out to get something for nothing.

Baloney. Most consumers have no problem paying for entertainment. One has only to look at the success of Fictionwise.com and the few other websites offering books and music at reasonable prices to understand that. If the music industry had a shred of sense, they'd have addressed this problem seven years ago, when people like Michael Camp were trying to obtain legitimate licenses for music online. Instead, the industry-wide attitude was *"It'll go away"*. That's the same attitude CBS Records had about rock 'n' roll when Mitch Miller was head of A&R. (And you wondered why they passed on The Beatles and The Rolling Stones.)

I don't blame the RIAA for Holling's attitude. They are, after all, the *Recording Industry* Association of America, formed so the labels would have a lobbying group in Washington. (In other words, they're permitted to make contributions to politicians and their parties.) But given that our industry's success is based on communication, the industry response to the Internet has been abysmal. Statements like the one above do nothing to help the cause.

Of course, communication has always been the artist's job, not the executives. That's why it's so scary when people like current NARAS president Michael Greene begin using shows like the Grammy Awards to drive their point home.

Grammy viewership hit a six-year low in 2002. Personally, I found the program so scintillating that it made me long for Rob Lowe dancing with Snow White, which at least was so bad that it was entertaining. Moves like the ridiculous Elton John-Eminem duet did little to make people want to watch again the next year. And we're not going to go into the Los Angeles Times' Pulitzer Prize-winning series on Greene and NARAS, where they pointed out that MusiCares has spent less than 10% of its revenue on disbursing emergency funds for people in the music industry (its primary purpose), or that Greene recorded his own album, pitched it to record executives while discussing Grammy business, then negotiated a $250,000 contract with Mercury Records for it (later withdrawn after the public flap). Or that NARAS quietly paid out at least $650,000 to settle a sexual harassment suit against him, a portion of which the non-profit Academy paid. Or that he's paid two million dollars a year, along with "perks" like his million-dollar country club membership and Mercedes. (Though it does make one wonder when he last entered a record store and bought something with his own hard-earned money.)

Let's just note that in his speech he told the viewing audience that NARAS and RIAA were, in large part, taking their stance to protect artists. He hired three teenagers to spend a couple of days doing nothing but downloading, and they managed to download "6,000 songs". Come on. For free "front-row seats" at the Grammys and an appearance on national TV, I'd download twice that amount! But...who's got time to download that many songs? Does Greene really think people out there are spending twelve hours a day downloading our music? If they are, they must be starving to death, because they're not making a living or going to school. How many of us can afford a T-1 line?

This sort of thing is indicative of the way statistics and information are being tossed around. It's dreadful to think that consumers are being asked to take responsibility for the industry's problems, which have been around far longer than the Internet. It's even worse to think that the consumer is being told they are

charged with protecting us, the artists, when our own industry squanders the dollars we earn on waste and personal vendettas.

Greene went on to say that "Many of the nominees here tonight, especially the new, less-established artists, are in immediate danger of being marginalized out of our business." Right. Any "new" artist who manages to make the Grammys has millions of dollars in record company money behind them. The "real" new artists aren't people you're going to see on national TV, or hear on most radio. They're people you'll hear because someone gave you a disc, or they opened at a show you attended, or were lucky enough to be featured on NPR or another program still open to playing records that aren't already hits.

As to artists being "marginalized out of our business," the only people being marginalized out are the employees of our Enron-minded record companies, who are being fired in droves because the higher-ups are incompetent.

And it's difficult to convince an educated audience that artists and record labels are about to go down the drain because they, the consumer, are downloading music. Particularly when they're paying $50-$125 apiece for concert tickets, and $15.99 for a new CD they know costs less than a couple of dollars to manufacture and distribute.

I suspect Greene thinks of downloaders as the equivalent of an old-style television drug dealer, lurking next to playgrounds, wearing big coats and whipping them open for wide-eyed children who then purchase black market CD's at generous prices.

What's the new industry byword? *Encryption*. They're going to make sure no one can copy CDs, even for themselves, or download them for free. Brilliant, except that it flouts previous court decisions about blank cassettes, blank videotapes, etc. And it pisses people off.

How many of you know that many car makers are now manufacturing all their CD players to also play DVD's? or that part of the encryption record companies are using doesn't allow your store-bought CD to be played on a DVD player, because that's the same technology as your computer? And if you've had trouble playing your own self-recorded copy of *O Brother Where Art Thou* in the car, it's because of this lunacy.

The industry's answer is to put on the label: "This audio CD is protected against unauthorized copying. It is designed to play in standard audio CD players and computers running Windows O/S; however, playback problems may be experienced. If you experience such problems, return this disc for a refund."

Now I ask you. After three or four experiences like that, *shlepping* to the store to buy it, then *shlepping* back to return it (and you still don't have your music), who's going to bother buying CD's?

The industry has been complaining for years about the stranglehold the middle-man has on their dollars, yet they wish to do nothing to offend those middle-men. (BMG has a strict policy for artists buying their own CDs to sell at concerts - $11 per CD. They know very well that most of us lose money if we have to pay that much; the point is to keep the big record stores happy by ensuring sales go to them. What actually happens is no sales to us *or* the stores.) NARAS and RIAA are moaning about the little mom & pop stores being shoved out of business; no one worked harder to shove them out than our own industry, which greeted every new Tower or mega-music store with glee, and offered steep discounts to Target and WalMart et al for stocking CDs. The Internet has zero to do with store closings and lowered sales.

And for those of us with major label contracts who *want* some of our music available for free downloading... well, the record companies own our masters, our outtakes, even our demos, and they won't allow it. Furthermore, they own our *voices* for the duration of the contract, so we can't even post a live track for downloading!

If you think about it, the music industry should be rejoicing at this new technological advance! Here's a fool-proof way to deliver music to millions who might otherwise never purchase a CD in a store. The cross-marketing opportunities are unbelievable. It's instantaneous, costs are minimal, shipping non-existant…a staggering vehicle for higher earnings and lower costs. Instead, they're running around like chickens with their heads cut off, bleeding on everyone and making no sense. As an alternative to encrypting everything, and tying up money for years (potentially decades) fighting consumer suits demanding their first amendment rights be protected (which have always gone to the consumer, as witness the availability of blank and unencrypted VHS tapes and casettes), why not take a tip from book publishers and writers?

Baen Free Library is one success story. SFWA is another. The SFWA site is one of the best out there for hands-on advice to writers, featuring in depth articles about everything from agent and publisher scams, to a continuously updated series of reports on various intellectual property issues. More important, many of the science fiction writers it represents have been heavily involved in the Internet since its inception. Each year, when the science fiction community votes for the Hugo and Nebula Awards (their equivalent of the Grammys), most of the works nominated are put on the site in their entirety, allowing voters *and* non-voters the opportunity to peruse them. Free. If you are a member or associate (at a nominal fee), you have access to even more works. The site is also full of links to members' own web pages and on-line stories, even when they aren't nominated for anything. Reading this material, again for free, allows browsers to figure out which writers they want to find more of - and buy their books. Wouldn't it be nice if all the records nominated for awards each year were available for free downloading, even if it were only the winners? People who hadn't bought the albums might actually listen to the singles, then go out and purchase the records.

I have no objection to Greene et al trying to protect the record labels, who are the ones fomenting this hysteria. RIAA is funded by them. NARAS is supported by them. *However, I object violently to the pretense that they are in any way doing this for our benefit.* If they really wanted to do something for the great majority of artists, who eke out a living against all odds, they could tackle some of the real issues facing us:

- The normal industry contract is for seven albums, with no end date, which would be considered at best indentured servitude (and at worst slavery) in any other business. In fact, it would be illegal.
- A label can shelve your project, then extend your contract by one more album because what you turned in was "commercially or artistically unacceptable". They alone determine that criteria.
- Singer-songwriters have to accept the "Controlled Composition Clause" (which dictates that they'll be paid only 75% of the rates set by Congress in publishing royalties) for any major or subsidiary label recording contract, or lose the contract. Simply put, the clause demanded by the labels provides that a) if you write your own songs, you will only be paid 3/4 of what Congress has told the record companies they must pay you, and b) if you co-write, you will use your "best efforts" to ensure that other songwriters accept the 75% rate as well. If they refuse, you must agree to make up the difference out of your share.
- Congressionally set writer/publisher royalties have risen from their 1960's high (2 cents per side) to a munificent 8 cents.
- Many of us began in the 50's and 60's; our records are still in release, and we're still being paid royalty rates of 2% (if anything) on them.
- If we're not songwriters, and not hugely successful commercially (as in platinum-plus), we don't make a dime off our recordings. Recording industry accounting procedures are right up there with films.
- Worse yet, when records go out-of-print, we don't get them back! We can't even take them to another company. Careers have been deliberately killed in this manner, with the record company refusing to release product or allow the artist to take it somewhere else.
- And because a record label "owns" your voice for the duration of the contract, you can't go somewhere else and re-record those same songs they turned down.
- And because of the re-record provision, even after your contract is over, you can't record those songs for someone else for years, and sometimes decades.

- Last but not least, America is the only country I am aware of that pays no live performance royalties to songwriters. In Europe, Japan, Australia, when you finish a show, you turn your set list in to the promoter, who files it with the appropriate organization, and then pays a small royalty per song to the writer. It costs the singer nothing, the rates are based on venue size, and it ensures that writers whose songs no longer get airplay, but are still performed widely, can continue receiving the benefit from those songs.

Additionally, we should be speaking up, and Congress should be listening. At this point they're only hearing from multi-platinum acts. What about someone like Ani Difranco, one of the most trusted voices in college entertainment today? What about those of us who live most of our lives outside the big corporate system, and who might have very different views on the subject?

There is *zero* evidence that material available for free online downloading is financially harming anyone. In fact, most of the hard evidence is to the contrary.

Greene and the RIAA are correct in one thing - these are times of great change in our industry. But at a time when there are arguably only four record labels left in America (Sony, AOL/Time/Warner, Universal, BMG - and where is the RICO act when we need it?)... when entire *genres* are glorifying the gangster mentality and losing their biggest voices to violence...when executives change positions as often as Zsa Zsa Gabor changed clothes, and "A&R" has become a euphemism for "Absent & Redundant"... well, we have other things to worry about.

It's absurd for us, as artists, to sanction - or countenance - the shutting down of something like this. It's sheer stupidity to rejoice at the Napster decision. Short-sighted, and ignorant.

Free exposure is practically a thing of the past for entertainers. Getting your record played at radio costs more money than most of us dream of ever earning. Free downloading gives a chance to every do-it-yourselfer out there. Every act that can't get signed to a major, for whatever reason, can reach literally millions of new listeners, enticing them to buy the CD and come to the concerts. Where else can a new act, or one that doesn't have a label deal, get that kind of exposure?

Please note that I am *not* advocating indiscriminate downloading without the artist's permission. I am *not* saying copyrights are meaningless. I am objecting to the RIAA spin that they are doing this to protect "the artists", and make us more money. I am annoyed that so many records I once owned are out of print, and the only place I could find them was Napster. Most of all, I'd like to see an end to the hysteria that causes a group like RIAA to spend over 45 million dollars in 2001 lobbying "on our behalf", when every record company out there is complaining that they have no money.

We'll turn into Microsoft if we're not careful, folks, insisting that any household wanting an extra copy for the car, the kids, or the portable CD player, has to go out and "license" multiple copies.

As artists, we have the ear of the masses. We have the trust of the masses. By speaking out in our concerts and in the press, we can do a great deal to damp this hysteria, and put the blame for the sad state of our industry right back where it belongs - in the laps of record companies, radio programmers, and our own apparent inability to organize ourselves in order to better our own lives - and those of our fans. If we don't take the reins, no one will.

Sources:
Baenbooks.com, BMG Records, Chicago Tribune, CNN.com, Congressional Record, Eonline.com, Grammy.com, LATimes.com, Newsweek, Radiocrow.com, RIAA.org, personal communications
* for more information on the Free Library, go to www.baen.com/library .

Attachment #4 – Janis Ian

FALLOUT - a follow up to The Internet Debacle

August 1, 2002

Author's note: You are welcome to post this article on any cooperating website, or in any print magazine, although we request that you include a link directed to
http://www.janisian.com
and writer's credit!

I. The original article

Quite frankly, when I spent three months researching and writing *The Internet Debacle*, I wasn't planning to become part of a "cause". I assumed that the 35,000 subscribers of *Performing Songwriter Magazine* might read it, and a few might email me about it. I had no idea that a scant month later, the article would be posted on over 1,000 sites, translated into nine languages, and have been featured on the BBC.

In the past twenty days I've received over 2,200 emails from unique senders. I've answered every one myself, getting an education I never intended to get in the process. I've corresponded with lawyers, high schoolers, state representatives, executives, and hackers. And I've felt out of my depth for a good portion of it.

I am in no way qualified to answer most of the questions I received, though I did my best, or referred them to someone else for discussion. The issues here are much, much bigger than I can encompass. I only wrote about downloading, record companies,and music consumers; within a few days, I found myself trying to answer questions like "Who owns the culture?" for myself. Length of copyright, fair use on the web, how libraries are being affected - these are all things I hadn't given much thought to before.

When I began researching the original article, I was undecided, but the more I researched, the more I reached the conclusions stated in the *Debacle* article. I've had only a few weeks since that article was published, and I've been on the road the entire time, so I haven't had the opportunity to research most of these questions. I want to thank Jim Burger and other attorneys and fans who kindly sent me articles and court cases to read off-line, while I was sitting in the car en route to the next city.

Do I still believe downloading is not harming the music industry? Yes, absolutely. Do I think consumers, once the industry starts making product they *want* to buy, will still buy even though they can download? Yes. Water is free, but a lot of us drink bottled water because it tastes better. You can get coffee at the office, but you're likely to go to Starbucks or the local espresso place, because it tastes better. When record companies start making CD's that offer consumers a *reason* to buy them, as illustrated by Kevin's email at the end of this article, we will buy them. The songs may be free on line, but the CD's will taste better.

II. My conclusions thus far:

"So why are the record labels taking such a hard line? My guess is that it's all about protecting their internet-challenged business model. Their profit comes from blockbuster artists. If the industry moved to a more varied ecology, independent labels and artists would thrive - to the detriment of the labels... The smoking gun comes from testimony of an RIAA-backed economist who told the government fee panel that a dramatic shakeout in Webcasting is 'inevitable and desirable because it will bring about market consolidation'." ("Labels to Net Radio: Die Now", Steven Levy in Newsweek, July 15, 2002.)

There are, as I see it, three operative issues that explain the entertainment industry's heavy-handed

response to the concept of downloading music from the Internet:

1. **Control.** The music industry is no different from any other huge corporation, be it Mobil Oil or the Catholic church. When faced with a new technology or a new product that will revolutionize their business, their response is predictable:

a. Destroy it. And if they cannot,
b. Control it. And if they cannot,
c. Control the consumer who wishes to use it, and the legislators and laws that are supposed to protect that consumer.

This is not unique to the entertainment industry. This mind-set is part of the fabric of our daily lives. Movie companies sued over VCR manufacturing and blank video sales, with Jack Valenti (Motion Picture Association of America chairman) testifying to Congress that the VCR is to the movie industry what the Boston Strangler is to a woman alone at night - and yet, video sales now account for more industry profit than movies themselves. When Semelweiss discovered that washing your hands before attending a woman in childbirth eliminated "childbed fever", at a time when over 50% of women giving birth in hospitals died of it, he was ridiculed by his peers, who refused to do it. No entrenched model has ever embraced a new technology (or idea) without suffering the attendant death throes.

2. ***Ennui.*** The industry is still operating under laws and concepts developed during the 1930's and 1940's, before cassettes, before boom boxes, before MP3 and file-sharing and the Internet. It's far easier to insist that all new technologies be judged under old laws, than to craft new laws that embrace all existing technologies. It's much easier to find a scapegoat, than to examine your own practices. As they say, "You can't get fired for saying no."

3. **The American Dream.** The promises all of us are made, tacitly or otherwise, throughout our lives as Americans. The dream we inherit as each successive generation enters grade school - that we will be freer than our grandparents, more successful than our parents, and build a better world for our own children. The promises made by our textbooks, our presidents, and our culture, throughout the course of our childhoods: Fair pay for a day's work, and the right to strike. The right to leave a job that doesn't satisfy, or is abusive. Freedom from indentured servitude. The premise that every citizen is allowed a vote, and no one will ever be called "slave" again. The promise that libraries and basic education in this country are free, and will stay so. These are not ideas I came up with on the spur of the moment; this is what we're taught, by the culture we grow up in. **And of everything we are taught, one issue is always paramount - in America, it is *the people* who rule.** It is *the people* who determine our government. *We* elect our legislators, so they will pass laws designed for *us*. *We* elect and pay the thousands of judges, policemen, civil servants who implement the laws we elect our officials to pass.
It is the promise that our government supports the will of *the people*, and not the will of big business, that makes this issue so damning - and at the same time, so hope-inspiring.
When Disney are permitted to threaten suit against two clowns who dare to make mice out of three balloons and call them "Mickey", the people are not a part of it. When Senator Hollings accepts hundreds of thousands of dollars in campaign contributions from entertainment conglomerates, then pretends money has nothing to do with his stance on downloading as he calls his own constituents "thieves", the people are not involved. When Representatives Berman and Coble introduce a bill allowing film studios and record companies to "disable, block or otherwise impair" your computer if they merely *suspect* you of file-trading, by inserting viruses and worms into your hard drive, it is the people who are imperiled. And when the CEO of RIAA commends this bill as an "innovative approach to combating the serious problem of Internet piracy," rather than admitting that it signifies a giant corporate step into a wasteland even our

government security agencies dare not enter unscathed, the people are not represented. (Hilary Rosen, in a statement quoted by Farhad Manjoo, Salon.com June 2002) *

III. A hopeful thought

"If classroom copying is sharply curtailed, if we give someone a software patent over basic functions, at some point the public domain will be so diminished that future creators will be prevented from creating because they won't be able to afford the raw materials they need. An intellectual property system has to insure that the fertile public domain is not converted into a fallow landscape of walled private plots." (James Boyle in the New York Times, March 31, 1996.)

I said that the research and information I've received over the past three weeks has made me hopeful, and I meant it. Because I know that although RIAA and their supporting companies can afford to spend 55 million dollars a year lobbying Congress and in the courts, they cannot afford to alienate every music buyer and artist out there. At that point, there will be a general strike, make no mistake. Just one week of people refusing to play the radio, buy product, or support our industry in any way, would flex muscles they have no idea are out there.

And I know that although businesses can spend unlimited dollars on campaign funding, only *the people* can elect a government. I believe that to a politician, no amount of lobbying money is worth the price of being voted out of office.

That, my friends, is why I have hope. Because I know that in America, votes count. Because I know that if enough people understand this issue, and vote accordingly, right will win. Legislation will be enacted that takes the will of the people into consideration, and favors their right to learn over Disney's right to control. Internet radio, currently in peril, will go offshore and out of the country if necessary, so audiences can hear thousands of songs instead of a narrow playlist. The RIAA will become a small footnote in the pages of Internet history, and the people will have triumphed - again.

A modest proposal for an experiment that might lead to a solution:

"The record companies created Napster by leaving a void for Napster to fill."
(Jon Hart and Jim Burger, Wall Street Journal [WSJ.com] April 2, 2001)

1. All the record companies get together and build a single giant website, with everything in their catalogues that's currently out of print available on it, and agree to experiment for one year.

This could be the experiment that settles the entire downloading question once and for all, with no danger to any of the parties involved. By using only out of print catalogue, record companies, songwriters, singers won't be losing money; the catalogue is just sitting in storage vaults right now. And fans can have the opportunity to put their money where their mouths are; if most people really *are* willing to pay a reasonable price for downloaded music, traffic on this site should be excellent. If most people really are downloading from sites like Napster because there's so much material unavailable in stores, traffic on this site should be unbelievably good.

*2. The site offers **only** downloads in this part of the experiment.*

Since all the items are unavailable on CD, there's no need to invest time and money linking to sites (or building record company sites) where consumers can buy them on a CD. This will also ensure that the experiment stays pure, and deals with only downloading. It would also preclude artists like myself from offering downloads of material available on CD's, skewing the results.

3. Here's where the difficult part comes in. *All the record companies agree that, for the sake of the experiment, and because these items are currently dead in the water anyway, they're going to charge a more-than-reasonable price for each download.*

By "reasonable" I'm not talking $1.50 per song; that's usurious when you can purchase a brand-new 17-song CD for a high price of $16.99, and a low price of $12.99. I mean something in the order of a *quarter per song*. I read a report recently showing that in the heyday of Napster, if record companies had agreed to charge just a *nickel* a download, they would have been splitting *$500,000 a day, 24 hours a day, 52 weeks a year.*
Record companies would have to agree that there'd be no limits on how many songs you could download, so long as you were willing to pay for each one; this is a major reason their own sites haven't been more successful.

4. Keeping the rate that low would:

a. Encourage consumers to use the site, even those of us for whom downloading with a modem is time-consuming and tedious.
b. Spread a lot of great old music around - and music, like all art, stands on the bones of those who've gone before. One of the big problems with so much catalogue out of print is that whole generations are growing up never having heard the "originals", but only the clones. It's always better to build on the real thing.
c. Do a great deal to repair the record companies' credibility in the eyes of consumers - in fact, it could be made to look like a gift of gratitude for all the support consumers have shown over the years! And while I know this may not seem important to the corporate model right now, it will become increasingly important as the world continues to shrink, mistrust of large business grows, and more and more people go back to "brand loyalty". If Sony are being reasonable, and BMG are not, sooner or later the Sony brand will conquer the market, and BMG will have to fall into line or fall out. That's capitalism at its best, isn't it?

5. Last but not least, the monies received would be portioned out fairly. I'm no economist, but the model might read something like this:

a. The record companies would bear the brunt of creating the site. There are plenty of ways for them to make money from this experiment, whether it works or not, and the massive exposure of their out of print catalogue, with a little attention to which albums receive the most downloads, could create a whole new sub-industry in a short time. It's good for them to share, and to pool their resources; if nothing else, it will stop their constant bickering for a while.
b. A reasonable (there's that word again) amount would be deducted off the top of each download to pay for costs. This would *not*, as is traditional, be borne completely by the artists or their heirs. It would be shared by all parties concerned - companies, singers, writers. Limits would be put on costs, so companies couldn't divert funds to pay their normal operating costs. And the accounts would be published *on the website monthly*, open for inspection by anyone. If you did this, they could even set up the initial experiment as a non-profit, and deduct the cost of putting up the site! Record companies would not be allowed to charge for storage fees, artwork, free goods to Guam; consumers could begin to trust them again.
c. From that point on, share and share alike. Let the record company, the artist, the songwriters and the publishers split the take equally. Don't laugh! The costs of that album are already paid, no matter what they tell you, and the only cost associated with this is putting the stuff on line, then maintaining the site itself. And again, the stuff was just sitting in storage; they weren't expecting any earnings from it. The songwriters, who traditionally get paid more than the singers, would be fairly compensated and have nothing to complain about. And the singers, for once, would be paid for the works they'd recorded.
d. In an ideal world, several different types of downloading formats would be available - wav. files, MP3 files, Ogg Vorbis files. Maybe you'd charge a tiny bit more for a higher sampling rate. And like the record companies, any companies owning the software for these downloads would donate their software for the sake of this experiment, with future terms to be negotiated later if it

> succeeds. What a great way for consumers to decide which one they like! What a great way for software companies to prove that theirs is better!

There are all kinds of other protocols you could implement once you knew whether this worked. For instance:

> 1. Imagine an Internet where there's one giant music site, easily accessible to anyone with a modem and computer. The site offers downloads at reasonable prices for everything and anything ever recorded, and links you back either to direct sales, or to other sites where you can purchase the music in CD, DVD, or other formats. Wouldn't it be great to search under an artist's name and literally be able to hear everything they ever did?
> 2. Links could be made from the artist and their work to press articles, streaming videos (I know, I know, but until we can all copy a stream to DVD as easily as we can from the TV to a video, it's a non-issue), special artwork, interviews, movies, concert footage, even guitar lessons.
> Live cams could show artist's concerts, from anywhere in the world, giving fans who can't go to Japan the opportunity to see how the concert is different there. Venues that maintain live cams could have their own sub-websites, and charge a fraction of the cost of going to a concert for these. They could even be coupled with tours of the surrounding area, interviews with local fans and artists, and the like. Who knows - the music industry might actually wind up educating an entire global generation. It won't affect concert sales, because people who go to a concert know they're getting something very different from sitting at home watching it on a screen. Otherwise, MTV and VH-1 would have put theaters out of business years ago.
> 3. Last and most important, artists and consumers could feel like they were a part of something bigger than themselves, and actually become *partners* with the music industry. And that industry, instead of responding with Draconian measures and safeguards, could feel like they were actually a part of the community - helping to further the artistic and intellectual resources of this country, and of the world.
>
> America has always exported its culture; that's our number one route into the hearts of the rest of the world. Instead of shutting that down, let's run with the new model, and be the first and the best at it. It's a brave new world out there, and somebody's going to grab it.

And now, on to the fun stuff:

Emails received: 1268 as of 07-30-02 (does not include message board posts)
Number of times the article has been translated into other languages: 9. (French, German, Chinese, Japanese, Italian, Spanish, Portuguese, Russian, Yugoslavian.)
Times AOL shut my account down for spamming, because I was trying to answer 40-50 emails at a time quickly and efficiently: 2
Winner of the *Put Your Money Where Your Mouth Is* award: Me. We began putting up free downloads around a week after the article came out. We will attempt to put up one free download a week for as long as we can - and leave them all up.
Change in merchandise sales after article posting (previous sales averaged over one year): Up 25%
Change in merchandise sales after beginning free downloads: Up 300%
Offers of server space to store downloads: 31
Offers to help me convert to Linux: 16
Offers to help convert our download files from MP3 to Ogg Vorbis: 9
Offers to publish a book expose of the music industry I should write: 5
Offers to publish a book expose of my life I should write: 3
Offers to ghost-write a book expose of my life I shouldn't write: 2
Offers of marriage: 1
Number of emails disagreeing with my position: 9
Number of people who reconsidered their disagreement after further discussion: 5

Interesting things about the emails: All but 3 were coherent. Of those, one only seemed to be incoherent,

but was in fact written by someone who spoke no English, and used Babblefish.com as a translator. (Sample: "I love your articles and play your music for my babies" became "I love babies and want to touch your articles.")
Silliest email: A songwriter who said he was going to download all my songs, burn them to CD's, and give them away to all his friends. Thank you!
Biggest irony: I'm writing this on a Sony Vaio laptop that came with my first ever CD burner, and easy instructions on how to copy a CD or download a file.

And from the emails:

"Several years ago the music industry reached an agreement with CD manufacturers to receive a royalty on blank, recordable CD's to compensate for the effects of copying music.. the recording industry is receiving a royalty for the "Audio" CD so that it can be used for copying music, taking the money, and then turning around and complaining that the CD is being used to make "unauthorized" copies. Now what is up with that? make up your mind!" (bohannon)

"...America On Line became so prominent by sending out CDs of their product via direct mail. Their growth rate quickly exceeded the capacity of their infrastructure, but that problem does not affect the music industry: they have the infrastructure. Why in the world do they not sign more small artists to a one-record deal, with "first-dibs" rights guaranteed to the record companies, for a comparatively small fee to the artist for the first record? They could send out CDs just the way AOL does, except with maybe 20 cuts per CD, of different artists, mailed quarterly? Eighty good artists per year, in your mailbox. If only one catches fire, the record company exercises their "first dibs" option, the artists can't bolt to a different label, and they get signed for a more standard record deal. Anyone who doesn't catch on gets dropped after one CD... at least they got a shot. Would the cost of this positive publicity really be any more than the cost of fighting file sharing?" (henry1)

"...they should take a tip from the movie industry and modern DVDs, which so overload the consumer with clear and compelling value that even those who wouldn't bat an eye about downloading a CD and not paying for it...have no motivation to spend dozens of hours downloading and piecing together all the value and quality available in a $25 DVD. I've bought DVDs for $20 where the movie was the tip of the iceberg--music tracks, documentaries, interactive presentations, audio tracks, stills, screen tests, and on and on....They can fight with compelling value--whether it's built in videos, computer games, free tickets, unique passwords to go download bonus tracks, demo tracks and dance mixes...karaoke tracks for each song, alternate vocal takes...Who could, or would, want to spend the time reproducing all that via downloading? As long as the consumer experience of a music CD can be duplicated with an hour or two of downloading and a quick burn to CD, they aren't going to convince anybody who might actually buy the CDs (but aren't, because they can download them) to do so...Rather than do things to alienate the current base of consumers that regularly buy their product, they should focus on adding value to their product." (kevin)

A final note:
Our representatives are not in Congress or the Senate because they want to make a better living. They're there because they want power, and influence. Without the office, they have neither.
*If they believe their actions will cause large amounts of the population to vote against them, **no** amount of money will be sufficient to buy their cooperation. If you let your representatives know, en masse, that you will not vote for them if they support ridiculous measures such as the bill allowing media companies to spread viruses on the computer of anyone "suspected" of file-sharing, and if enough of you tell them so, they will NOT work hand in glove with the RIAA.*
We cannot possibly match the monies the record companies can devote to litigation, but we CAN threaten to vote those representatives who are in bed with them out of office. And ultimately, it's the votes they care about.

* The article describing this bill can be found at http://news.com.com/2100-1023-945923.html?tag=fd_lede

PREPARED STATEMENT OF THE NATIONAL MUSIC PUBLISHERS' ASSOCIATION

On September 26, 2002, the Subcommittee held a hearing "Piracy Of Intellectual Property On Peer-to-Peer Networks, in which H.R. 5211, the Peer-to-Peer Piracy Prevention Act was discussed at length. The National Music Publishers' Association (NMPA) appreciates this opportunity to submit written comments on this important subject.

NMPA works to protect and advance the interests of the music publishing industry. With more than 800 members, NMPA represents the leading companies in the industry, from those affiliated with large media companies to the industry's largest and most influential independent music publishers The Harry Fox Agency, NMPA's licensing affiliate, provides an information source, clearinghouse, and monitoring service for licensing music copyrights and acts as licensing agent for more than 27,000 music publisher-principals, who in turn represent more than 160,000 songwriters.

NMPA applauds the subcommittee for focusing on the pressing problem of peer-to-peer piracy. As evidenced by the Napster litigation, peer-to-peer piracy has since its inception posed a serious threat to music copyright. The International Federation of the Phonographic Industry (IFPI) observed that the U.S. music sales market experienced a 9.4% decline in 2001, with Internet infringement and CD burning two of the principle responsible factors. In the year 2000, international enforcement actions taken by IFPI and its 46 national affiliates led to 15,000 websites containing 300,000 files being taken down. There is no question that illegal file-sharing is a substantial portion of the digital infringement problem. In November of 2001, NMPA and several songwriters filed a class-action copyright-infringement suit in Los Angeles against the operators of the Morpehus, Grokster and KaZaA file-sharing systems, following a suit in October of that year by the Recording Industry Association of America and the Motion Picture Association of America. A positive decision was recently obtained against the Aimster system, while the litigation against Morpheus, Grokster and KaZaA is still pending. The substantial problems of peer-to-peer piracy remain. The attention of the subcommittee to the serious nature of this problem is therefore greatly appreciated.

H.R. 5211 would authorize copyright owners to utilize technological self-help measures to prevent unauthorized distribution of copyrighted works over peer-to-peer networks. The authorization is meant to relieve copyright owners from the specter of liability under certain common law doctrines and state and federal statutes, including the federal Computer Fraud and Abuse Act, when they use self-help measures such as interdiction, decoy, redirection, spoofing and file-blocking. At the same time, it provides a new federal cause of action against copyright owners who abuse their right to use self-help measures. NMPA supports the legislation's laudable goals of protecting the use of reasonable measures by copyright owners. At the same time, NMPA would like to see certain clarifications and modifications to the bill.

NMPA's first issue relates to the preemptive effect of the bill. As currently written, the bill preempts causes of action under state laws only when the copyright owner's self-help actions are in compliance with the standards of the bill. If a copyright owner unknowingly exceeds the boundaries of H.R. 5211 and causes, for example, $300 worth of damage to computer files or data, the copyright owner could be sued under state laws that may have very different (and much lower) substantive standards for finding a violation, and very different (and much higher) potential for damage awards. For example, simply imposing a burden on the finite capacity of a computer has been found to be sufficient damage under some state law theories. In the context of spamming and misleading advertising, such a rule may be reasonable, but the rule has not been clearly limited to those types of behavior. Even if the copyright owner prevails, which we believe is a distinct possibility, the burden and expense of state litigation will have been borne—which we believe is unfair and unnecessary in this situation.

NMPA believes that a more appropriate and customary approach to preemption would be for the federal law to preempt state laws in all instances. Such an approach is supported by the fact that peer-to-peer networks and the communications over them are by their nature interstate. Accordingly, a single federal cause of action with an appropriate remedy that balances the interests of those concerned is preferred to a patchwork of potentially inconsistent and inappropriate state laws.

The fact that the subject of the bill is copyright law also argues in favor of a single federal law that broadly preempts state causes of action and remedies. The basis for copyright statutes lies in the U.S. Constitution. Section 301 of the Copyright Act preempts state laws that are equivalent to copyright, thus limiting the rights of those who create intellectual property. It would be unfair to deprive copyright own-

ers of the benefit of state laws while providing those who infringe on federal copyrights the ability to use state laws against copyright owners.

Although not strictly an issue of preemption, the preference for a single cause of action also means that the bill should be clear that no cause of action exists under the Federal Computer Fraud and Abuse Act against copyright owners who seek to protect their rights under federal copyright law by engaging in interdiction, decoy, redirection, spoofing and file-blocking. The federal courts have given the CFAA a broad reading, finding "damage" to computer files or data to include any impairment of the integrity or availability of computer programs or data. One court has found "impairment" to occur when a large volume of unsolicited bulk email causes slowdowns or diminishes the capacity of a service provider. Under this reading, it is possible that some of the legitimate anti-P2P piracy techniques—including decoy, redirection and spoofing—could result in slowing down the computer of the file trader, in which case a claim under the CFAA might be brought. As noted with state causes of action, while the copyright owner may prevail under the CFAA, it will have borne the burden and expense of additional litigation. The CFAA should therefore be superseded by H.R. 5211 when copyright owners engage in legitimate anti-piracy efforts under the bill.

The second point of concern to NMPA is the notice requirement. The present draft of the bill requires that the copyright owner give notice to the Department of Justice of "the specific technologies the copyright owner intends to use to impair the unauthorized distribution, display, performance, or reproduction of the owner's copyrighted works over a publicly accessible peer-to-peer file trading network". It is somewhat unclear whether this notice must be given every time that a particular technology is to be used, or only the first time. We encourage clarification that the notice is required only upon the first use of a technology.

Third, NMPA would like to address what has been characterized as a "safe harbor" provision in the bill. The nature of a safe harbor is that a potential defendant should be assured that its actions will not expose it to liability if it complies with an objective, mechanical bright-line test of unambiguous requirements that exempt it from the a prima facie cause of action under the statute in question. Subsection (c) of the bill,—which states that "A copyright owner shall not be liable under subsection (a) for an act to which subsection (a) applies" if the copyright owner complies with the provisions regarding notice to the Department of Justice and the affected file trader—has been presented as a safe harbor. Subsection (a) of the bill, however, states that the copyright owner shall not be liable if its actions do not "alter, delete, or otherwise impair the integrity of any computer file or data residing on the computer of a file trader". Thus, the cross-reference to subsection (a) that appears in subsection (c) appears to provide that notice to the Department of Justice and the affected file trader is not sufficient to bring the copyright owner within the protection of the safe harbor. Rather, the safe harbor only applies if the notification requirements are met and the act of the copyright owner does not alter, delete, or otherwise impair the integrity of any computer file or data residing on the computer of a file trader. This is not a standard safe harbor, since it effectively says that the copyright owner will not be liable for causing harm if it does not cause harm.

Simply satisfying the notification requirements should be sufficient to put the copyright owner within the safe harbor, unless it can be shown that the copyright owner intended that harm to computer files or data would result. This formulation of the safe harbor would promote the filing of notice, provide the Department of Justice with information about the various self-help technologies being used, protect copyright owners from liability if unintentional or unforeseen harm to a computer file results, but deny protection to copyright owners that knowingly or intentionally cause harm to computer files or data. We believe this strikes the proper public policy balance.

NMPA's comments should be viewed within the context of its overall support for the intent of this legislation, which addresses one of the most profound and serious threats today to the rights of copyright owners. NMPA appreciates the subcommittee's efforts in this area and looks forward to continued participation in the consideration of this issue and this particular piece of legislation. Thank you for this opportunity to express our views.

September 25, 2002

Chairman Howard Coble
Subcommittee on Courts, the Internet, and Intellectual Property
Committee on the Judiciary
United States House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

Subject : Oversight Hearing on "Piracy of Intellectual Property on Peer-to-Peer Networks"

Dear Chairman Coble and Committee Members,

We appreciate the opportunity to contribute to the ongoing dialogue regarding piracy of intellectual property over peer-to-peer networks. As the world's largest semiconductor company and a major technology and building block supplier to the Internet economy, we have a direct interest in the development and deployment of revolutionary technologies that advance global computing and communications capabilities and enhance network build-out. To that end, we want to make sure that Congress understands that peer-to-peer technologies are not simply a sub-culture phenomenon developed for specific use in illegal redistribution of intellectual property. To be sure, digital piracy threatens not only the copyright industries, but also the emergence and effectiveness of exciting new digital markets; the fabric of emerging global electronic commerce. As a company founded on intellectual property, Intel in no way condones intellectual property theft, but we have great concern with efforts to stigmatize and threaten technologies based solely on the selective few who may use technology in harmful ways.

The Promise of Peer-to-Peer Technology

In its most basic form, peer-to-peer technology is a revolutionary architectural approach to resolving inherent weaknesses in traditional client/server computing architectures, where the functionality of the environment is dependent upon a limited number of physical servers. This server dependency creates a concentrated point of architectural vulnerability and bottleneck to distributed computing efficiency. Computer scientists have been working for over thirty years to increase network architecture efficiencies by expanding the role of individual network nodes. These efforts have spawned entirely new architectures for distributed and workgroup computing, and today, peer-to-peer technologies are the foundation for a class of exciting productivity applications widely deployed throughout enterprises and the Internet (E-mail, Microsoft Windows for Workgroups, Lotus Notes)

Intel has long recognized that peer-to-peer computing technologies provide a foundation for many incredibly productive applications that can bring exponential storage, computing and communications power to our increasingly networked digital world.[1] For example, Intel has been using peer-to-peer technologies for years to connect thousands of engineering PCs together to simulate new chip designs. Not only has this increased Intel's collective computing power, it has resulted in cost savings of many millions of dollars. As another example, the Intel® Philanthropic Peer to Peer Program employs the connected PC and the power of peer-to-peer technology to significantly increase computing capabilities for researchers seeking cures for leukemia and other forms of cancer. But Intel is not alone. Peer-to-peer technologies are enabling other legitimate new businesses and collective research activities, which harness the collective computing power of millions of PCs around the world in pursuit of a common good. [2] We have only scratched the surface of the benefits that peer-to-peer technologies are capable of bringing to the lives of whole generations of connected businesses and consumers.

Technology Mandates Cannot Replace Personal Responsibility and Law Enforcement

Although Intel understands that peer-to-peer technologies, *like all other useful and productive tools,* have the potential for misuse (e.g., unauthorized sharing of copyrighted works), there is *nothing inherently bad* about peer-to peer-technologies themselves (in fact, quite the opposite). Yet, as many have engaged in the debate regarding services like Napster, Kazaa and Morpheus, the distinction between peer-to-peer technologies generally, and these specific services, has largely gotten lost. In this context, while Intel supports the right of content providers to protect their intellectual property through enforcement actions that place liability directly with infringers, we oppose efforts that put whole classes of neutral technologies on trial. Associating a broad class of technologies with the specific applications employed by opportunists runs the risk of replacing personal responsibility and law enforcement with technology mandates of Orwellian magnitude. We cannot let this happen. Technology mandates simply cannot replace personal responsibility and law enforcement in an ordered society. Not only does this course of action threaten the continued advance of technology, it threatens the continued advance of an enlightened digital culture.

"Self Help" Cannot Interfere with Individual Privacy and Security

We have recently had the opportunity to consider legislative proposals that would legalize "self help" efforts to combat digital piracy that occurs over certain peer-to-peer

---

[1] Many peer-to-peer networking technologies have technical advantages over server-centric technologies for critical communications, collaboration and even intellectual property protection. For example, peer to peer technologies can enable computing, storage and server capabilities on scales of magnitude larger than many traditional technologies at a fraction of the cost, and its distributed computing capabilities can be used to enhance reliability & robustness.

[2] Peer to peer technologies enable countless "content-neutral" business and social opportunities, such as: secure communication and collaboration among small groups, a.k.a. "groupware" (*e.g.*, Groove, Ikimbo, and Magi Enterprise); online marketplaces and supply chains (*e.g.*, FirstPeer); online education and distance learning (*e.g.*, Colloquia); secure health care information exchange (*e.g.*, CareScience); Intra- and inter-organizational content and knowledge management (*e.g.*, NextPage); distributed computing (*e.g.*, SETI@Home); messaging (*e.g.*, Jabber and Apple's Rendezvous); computer games (*e.g.*, Quazal); secure distribution of licensed media and intellectual property (*e.g.*, Akamai and RightsMarket, Inc.); for other examples, see (http://www.openp2p.com/pub/q/p2p_category).

networks. While we generally support reasonable self-help to protect intellectual property, we do not believe intellectual property self-help is superior to the rights of legitimate businesses and individuals to be secure in their persons and property. We are therefore inherently skeptical of laws that seek to make legal or create safe harbors for self-help measures that might harm or jeopardize these fundamental rights, or that might deter the legitimate development and deployment of exciting new technologies like peer-to-peer. We are therefore greatly concerned about the implications, both short and long term, of any proposed law that would (our could be construed to) (i) authorize general attacks on systems as opposed to reasonable interference with a specifically known unlawful activity on a peer-to-peer network; the primary purpose and function of which is to enable unauthorized file sharing; (2) provide immunity for any damage beyond interference with the specifically known unlawful activity on such network; (3) undermine current laws against cyber crime, including but not limited the Computer Fraud and Abuse Act; and (4) otherwise interfere with the lawful activities of legitimate peer-to-peer businesses and users. We hope that Congress will similarly be skeptical of any such proposals and apply a heightened level of scrutiny to them.

Summary and Conclusions

In closing, we ask Congress to remember that peer-to-peer is not a "thing" that is inherently good or bad; it is a fundamental technology and capability of the Internet, like the Internet Protocol (IP). Congress should not let the opportunistic misuse of this exciting capability lead to the adoption of laws that (i) seek to replace personal responsibility and enforcement of existing laws with technology mandates or (ii) undermine the legitimate rights of privacy and security. In short, we recognize that infringers should stand trial as appropriate, but technologies should not. We hope that Congress will therefore view with skepticism and heightened scrutiny any proposal that has the potential of enabling self-help measures to undermine individual privacy and security and the advancement of technology.

Respectfully submitted,

Donald M. Whiteside
VP Legal & Government Affairs
Intel Corporation

PREPARED STATEMENT OF STEVE GRIFFIN

What is peer-to-peer? What are its uses? Who uses peer-to-peer? What kind of company is StreamCast Networks? What kind of company was Napster? These are important questions and the answers need to be understood by Members thinking about legislating in an area that impacts their constituents and peer-to-peer. Considering that no true technology companies or interests are present at the hearing—it is clear that there is not an understanding of peer-to-peer. Without an idea of what the technology does, a premature, incorrect assumption may be growing on the Hill that all peer-to-peer software and technology is destined to be enjoined by the Courts (i.e., they improperly only think of the now defunct Napster or Aimster when completely different Peer-to-Peer software tools exist). It is as if Members categorically presume innovative peer-to-peer products are illegal despite such software products' respective uniqueness; this notwithstanding the fact that such a determination has not been established in a court of law in proceedings currently pending regarding decentralized peer-to-peer technologies. The challenge today is overcome the scare tactics and resist creating a temporary or shortsighted fix that is neither in the best interest of the public or in favor of the innovation of technology.

What I have found in the many years in business and 27 years of marriage is that the most important action to overcoming challenges is working together to find common ground. Rather than fighting, suing and hacking like the content industry is doing, I am spending my energy trying to find solutions that benefit everyone including content creators, content owners, consumers and content communicators. The solution will only come when all the stakeholders sit down together in effort to attempt to reach a reasonable, workable resolution to the on-going battle between content and technology.

WHAT IS PEER-TO-PEER?

Peer-to-Peer, commonly referred to as "P2P", is a communications model in which each party has the same capabilities and either party can initiate a communication session. In some cases, peer-to-peer communications is implemented by giving each communication node, otherwise known as a user, both server and client capabilities. In recent usage, peer-to-peer has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server.

WHAT IS PEER-TO-PEER TECHNOLOGY?

Collaborative computing, also known as distributed computing, pools the processing power of multiple computers. Instant messaging applications like Morpheus Messenger, MSN Messenger and AOL Instant Messenger, allow users to swap messages and files synchronously. This allows people to use shared space in which they interact directly without dealing with servers and boundaries, doing things such as collaborating on documents in a shared space and searching each others' computers and shared folders, also called file sharing.

WHAT IS PEER-TO-PEER SOFTWARE?

A true P2P software product, like Morpheus, allows consumers to connect directly with each other and to exchange any type of information—anything—recipes, family photographs, a poem from a budding poet, commentary on public issues, anything. Once consumers have downloaded the Morpheus software they choose what electronic information that they want to make available to people around the world. In short, Morpheus allows consumers to directly connect to each other like the Internet was intended to be—a communication tool where users are both senders and receivers of information. It is a new gateway or alternative to the World Wide Web where users have primarily been only receivers of data (i.e., visiting a company's website to obtain information on that company provided to the site visitor by that company).

P2P'S BENEFITS INCLUDE, BUT ARE NOT LIMITED TO:

1. Businesses worldwide can save billions by using distributed computing setups that take advantage of unused bandwidth and resources.
2. P2P knocks down the barriers to publishing, communicating and sharing information.
3. P2P permits easier access to all types of data, files and information.
4. P2P provides content creators with a venue to communicate and share ideas and information directly.

SOCIETAL IMPACT OF PEER-TO-PEER

The reason that I am so passionate about the Peer-to-Peer technology platform is that it not only can lead to important societal changes but also itself reflects important societal changes that have already taken place. Individuals—on their own, unaided by the communications giants—are finding their own new ways of connecting, of communicating, and of creating and controlling their own communication channels. Their will—connected and empowered—is prevailing now and Congress should not overlook them.

The old Internet, or the way that it has been since 1996, was and remains a distribution channel that has been controlled by traditional companies where users were primarily receivers of information. With the "New Internet" consumers are not merely receivers of information, they are also senders. StreamCast Networks is committed to incorporating different tools that empower consumers to communicate and exchange information directly with one another.

USERS OF PEER-TO-PEER TECHNOLOGY

The Morpheus software program is a communication tool that allows users to independently connect to one another to form a user network, commonly known as a user-to-user or "peer-to-peer" network. Using Peer-to-Peer networking functionality of the software, users may search for and compare any kind of computer file, including text, images, audio, video, and software files with other computer users running similar networking software. With Peer-to-Peer software such as Morpheus, the searching and file-sharing functions are entirely decentralized—after downloading and installing the Morpheus software on their computers, users decide for themselves what information to seek out, send and receive with the software, without any further involvement from StreamCast.

Something that needs to be understood by the Members is that contrary to what has been incorrectly depicted in some media reports or by major motion picture companies and major recording labels, Morpheus is *not* the same as Napster nor does the Morpheus software work the same way Napster's service operated. Napster provided a service that directly helped its users find specific copyrighted songs. StreamCast provides no such service, but merely provides a Peer-to-Peer *software* tool called Morpheus that permits users of the software to connect directly and form a decentralized user network. In contrast to Napster, StreamCast does not operate any user network, and it does not operate a file-indexing service. Users of the Morpheus software program take advantage of the program's full file-sharing functionality without StreamCast's continued involvement. Users join the user network, select which files to share, send and receive searches, and download files, all without the involvement of StreamCast.

TECHNOLOGICAL INNOVATION AND THE BENEFITS OF P2P TECHNOLOGY

Unlike the media-conglomerates, consumers are not resisting change; they are encouraging and embracing it. They are clear about wanting commercial content available and wanting to create content to share as well as wanting a broadband connection. Like e-mail products before it, Peer-to-Peer communication tools are likely to drive the next wave of technology buying in the home and office.

The rise of Peer-to-Peer networking is part of a long-standing historical trend in technological innovation: the migration of ever-more powerful publishing tools in the hands of individuals. The trend has been driven of obvious marketplace demand and individuals desire for tools that enable creation, reproduction and distribution of information.

There is little debate that consumers around the world represent an incredible opportunity to release creative expression. Decentralized P2P offers the most cost effective and efficient distribution platform that exists today. By leveraging millions of consumers' computers and their distributed bandwidth, enormous cost of goods savings are realized. For instance, when consumers launch the Morpheus P2P software, they join and help create a self-organizing, self-sustaining network of users around the world. The more users that join the network and share content, the richer the experience is for everyone.

Consumer demand has spurred technological innovation that has delivered enormous benefits, both for society at large and copyright holders. Virtually every American has enjoyed the benefits brought by the audio-cassette recorder, the photocopier, the VCR, the personal computer, and the Internet. The copyright industries, meanwhile, have seen the size of their own markets, as well as the value of their content libraries, increase in part due to the new markets opened up by these new consumer technologies. Over the last century, new technologies and copyrighted

works have been complementary—advances in the former have, over time, invariably increased the value of the latter.

Bearing in mind the enormous benefits of P2P available now and in the future, I urge you to consider the new threat to consumer's freedom and privacy, as well as to the future of the Internet. Technology issues are difficult to get ones hands around, believe me as a CEO trying to make a new species of business work I understand the complexity of the situation the Committee is in. On one side you are being asked by multi-national media conglomerates to control consumer behavior and their use of various products and information like computers, personal listening devices and stereos. Rather than provide the consumer with a reasonable solution to consumer demand, the media companies have decided to sue the consumer directly arguably to force them 'back into line" as well as have requested Congress give them the ability to hack computers used by their consumers who use Peer-to-Peer software products. Then on the other side are innovative technology companies that are creating technologies that need time to mature and be adopted by the mainstream public. Let's not forget the driving force of this unfortunate battle between content owners and technology companies, the consumers, who are caught in the crossfire.

THE HISTORY OF THE BATTLE BETWEEN TECHNOLOGY AND CONTENT

The battle over technology vs. content is nothing new. While it is natural to resist change, it is necessary for growth.

History proves to be a valuable teacher. The content industries have repeatedly tried to repress new technologies. By way of example, piano rolls, radios, cassette recorders, VCRs, Digital Audio Tape, MP3 players, cable television, in-room video, and Replay TV were each met with content industries' pessimistic pronouncements of gloom and doom and efforts to outlaw them. Fortunately, Courts have been reluctant to grant copyright owners the power to prevent technological innovation in order to gain control over their copyrights. Likewise Congress should continue to refrain from granting copyright owners the power to stifle new technologies. History proves that such technological innovations have not only made America and the world a better place, but have made the content industries and copyright holders richer too.

This ongoing battle is best described in relation to the Betamax lawsuit in the 1980s in which two movie studios filed a lawsuit hoping to stop the manufacturing and distribution of Sony Betamax VCRs.

At the time, Jack Valenti, who heads the Motion Picture Association of America, went so far as to declare, "the VCR is to the American film producer and the American public as the Boston Strangler is to the woman home alone." Fortunately for consumers and businesses alike, the Supreme Court of the United States sided with Sony. Not only did the sales of VCR boom, but also a flood of new revenue streams for Hollywood was created.

In the 1940s, when radio was still considered a technological innovation by many American consumers, copyright holders were not being paid but consumers were nonetheless able to enjoy music for free. This technology first was used in homes and offices and eventually migrated to a mobile device, the automobile—a migration not too different from digital music's route from desktops to MP3 players.

Congress might have responded as Congressman Berman now suggests by allowing the copyright holders to attack the owners and users of radios. They could have passed a law that allows copyright holders to interdict, redirect, decoy, spoof, and signal-block or jam the radio airwaves preventing music from reaching consumers' radios.

Fortunately, no such law was passed.

Had Congress permitted content owners to block or otherwise sabotage radio airwaves, radio might not exist as we know it today. In this situation, a very direct correlation exists where you as elected representatives can determine a successful outcome of the struggle for content owners trying to keep up with the pace of technological innovation.

Congress has repeatedly stepped in to arbitrate between new technologies and copyright law. On some occasions, Congress has created compulsory licenses to mediate the tension. On other occasions, Congress has resisted entirely the demands of the copyright industries for control over new technologies. Today, there is no more cause to curb peer-to-peer technology in the name of preventing so-called "piracy" than there was to stop the VCR or radio.

CURRENT PROPOSALS

The legislative proposals on the table clearly do not have the consumer or the majority of content creators in mind and are neither reasonable nor workable.

Senator Fritz Hollings introduced legislation along with five cosponsors on March 21, 2002. The Consumer Broadband and Digital Television Promotion Act is a bill to regulate interstate commerce in certain devices by providing for private sector development of technological protection measures to be implemented and enforced by Federal regulations to protect digital content and promote broadband as well as the transition to digital television, and for other purposes. Because it essentially mandates that hardware be built according to the terms of multinational media companies instead of the technology companies creating the product to meet consumer demands, Senator Hollings' proposal would be devastating to the future of innovation and entrepreneurship around the world.

Over the past several months, multiple news services have reported that major record labels have launched an aggressive new guerrilla assault on the file-sharing networks by flooding online sharing networks with bogus copies of popular songs. Yet, it appears that Hollywood recognizes that such tactics may run afoul of state and federal laws, requesting that Congressman Howard Berman (D-CA) introduce legislation that would legalize their illegal actions.

H.R. 5211 allows copyright owners to employ the methods of hackers such as interdiction, redirection, decoys, spoofing, and file-blocking. It not only proposes granting copyright owners a 'safe harbor' from current state and federal laws, but also essentially makes copyright owners the proverbial 'long arm of the law' to self-enforce rules set by the government without meaningful remedy for abuse of the rights requested in the legislation.

It is interesting that Congressman Berman has chosen the end of session to introduce H.R. 5211 which would hobble a technology at the same time saying, ". . . P2P represents an efficient method of information transfer and supports a variety of legitimate business models. Removal of all P2P networks would stifle innovation." Further, it is at a time when analysts such as Josh Bernoff at Forester Research report that "[T]here is no denying that times are tough for the music business, but not because of downloading".

It appears that a goal of the content industries who support The Consumer Broadband and Digital Television Promotion Act and/or Congressman Berman's H.R. 5211 is simply to prevent the development of any technology—including the Internet—that is not designed or organized to maximize their own profits or to control so-called, "piracy"; this despite the fact that history has consistently shown that suppression of technology is shortsighted.

It is important to remember that the content industries do not represent all copyright holders or the public interest. Clearly, content industries desire laws to maximize their profits and without regard to how the public and other industries may be affected. Furthermore, to give one industry, namely the multi-media conglomerates, no matter how large and well-funded, the power to control innovation that affects countless other industries, would undermine the free flow of commerce that has brought the U.S. all the fruits of technological innovation.

CONCLUSION

StreamCast believes that there is an array of reasonable solutions to the battle between the content industry and the technology industry over such issues as Peer-to-Peer technology and use. Rather than adopt shortsighted, nonsensical, and overreaching laws like the ones suggested by Congressman Berman and Senator Hollings, Congress should facilitate a dialogue between the stakeholders in an effort to reach a reasonable, workable solution to these very important issues. If this fails to happen, the ordinary citizen, the consumer, is the one who will ultimately lose.

News *Release*

AMERICAN LEGISLATIVE EXCHANGE COUNCIL

For Immediate Release
September 26, 2002

Contact:
David Wargin (202) 466-3800

ALEC Supports Verizon's Right to Protect Consumer Privacy

Washington, D.C., September 26, 2002 -- The American Legislative Exchange Council (ALEC) urges a federal court in Washington, D.C. to prevent the Recording Industry Association of America (RIAA) from forcing Verizon to release the identity of one of its customers.

The controversy stems from the RIAA using the Digital Millennium Copyright Act (DMCA) to ask a federal court to enforce a subpoena requiring Verizon to release the identity of one of its customers. The law, enacted by Congress in 1998, is an update to the U.S. copyright laws for the digital age. But the RIAA is not using the law as it was originally intended.

"DMCA does not create a class of property that is superior to tangible property," said Morgan Hayley Long, Director of ALEC's Telecommunications and Information Technology Task Force. "The property interests of RIAA are of no less significant constitutionally and statutorily than that of Verizon's own property rights and the property rights of its customers."

"The ramifications are immense – affecting the privacy rights of millions of everyday Internet users," added Long. "If RIAA is granted their request, the court will be making a sweeping legal precedent that would not only establish a hierarchy for property rights, but also endanger consumers' privacy rights."

The American Legislative Exchange Council is the nation's largest, bipartisan membership organization of state legislators. The Telecommunications and Information Technology Task Force seeks to improve America's competitiveness through innovative free market policies.

-30-

September 26, 2002

The Honorable Howard Coble
Chairman
House Committee on the Judiciary
Subcommittee on Courts, the Internet, and Intellectual Property
B351A Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Coble:

As the Co-Chairs of USACM, the U.S. Public Policy Committee of the Association for Computing Machinery, we are writing to express the strong concerns of the computing community regarding H.R. 5211, the P2P Piracy Prevention Act. Please include this letter in the official record of the subcommittee's September 26 hearing entitled "Piracy Of Intellectual Property On Peer-to-Peer Networks."

As a professional association that promotes both technical and ethical excellence in computing, we are concerned that H.R. 5211 would legitimize a variety of questionable acts that violate professional and ethical standards. An essential aim of computing professionals is to minimize negative consequences of computing systems. Sanctioning the use of computing technology in the intentional destruction or modification of files and programs sets a dangerous precedent that conflicts with the responsibilities and expectations of professional conduct. This contradiction is especially troubling for professionals involved in computing education.

Of particular concern to the computing community, H.R. 5211 makes a number of flawed technical assumptions and includes a set of ambiguous definitions that would result in a variety of unintended consequences harmful to the use and continued development of the Internet. The following are just a small sampling of our concerns with the legislation:

*The definition of a "peer-to-peer public network" seems to include all computers connected to the Internet as well as fundamental software applications such as email and WWW service.

* Legally encouraged interdiction, spoofing, redirection, and denial-of-service attacks would create new volumes of network traffic resulting in Internet service disruptions and degradation of service for innocent Internet users, many of whom may not be using P2P networks. Such uses include electronic commerce transactions and a variety of research, education, free speech, health care, and other noncommercial activities.

*The legislation underestimates the technical challenge in targeting an attack at a specific copyrighted work without causing collateral damage to others through a shared connection, server, or repository of personal and business files.

*Legally sanctioned attacks would involve defeating legitimate security mechanisms and firewalls. This approach conflicts with efforts to enhance cybersecurity and seems to violate the anticircumvention provisions of the Digital Millennium Copyright Act and prohibitions in the USA Patriot Act.

*The legislation does not recognize that P2P networking protocols are used for a variety of purposes. Research and development conducted using P2P shows great promise for inexpensive yet powerful distributed

computation.

As an international association with members in over 100 countries, we are also concerned with the international implications of H.R. 5211. As we have learned through the complicated negotiations over the Council of Europe Cybercrime Convention and the Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters, countries have diverse cultural expectations of the Internet. Clearly, H.R. 5211 would affect many people who are not under the jurisdiction of U.S. laws. It would be unfortunate if other countries were to use this legislation to sanction attacks on U.S. based content that they find to be objectionable.

The scientists, educators, artists, publishers, and other computing professionals of ACM have major interests in copyright. We are concerned about the protection of our property, but we are addressing this challenge through the investigation of new business models and methods better suited to a "wired" world. The small segment of U.S. industry that would benefit from H.R. 5211 - namely entertainment companies - will continue to face challenges in a rapidly changing global market place until they adopt similar changes. Legislative efforts that encourage vigilante attacks on P2P networks are not the answer, but only serve as an invitation for additional problems at the expense of society at-large.

USACM is pleased to offer our technical expertise to assist policymakers in the development of legislation of concern to the computing community. Please contact the ACM Office of Public Policy at (202) 478-6312 if we can provide additional information.

Sincerely,

Barbara Simons, Ph.D.
Eugene H. Spafford, Ph.D.

Co-Chairs
U.S. ACM Public Policy Committee (USACM)
Association for Computing Machinery

Cc: Members of the House Committee on the Judiciary

The Register of Copyrights
of the
United States of America

Library of Congress
Department 17
Washington, D.C. 20540

(202) 707-8350

September 25, 2002

RE: Hearing on Piracy of Intellectual Property on Peer-to-Peer Networks

Dear Representative Berman:

In response to your request, I am responding to an assertion made in written testimony for tomorrow's Subcommittee hearing on "Piracy of Intellectual Property on Peer-to-Peer Networks" that U.S. copyright law does not give copyright owners a separate exclusive right of "making available."

This statement reflects an incorrect understanding of U.S. copyright law. While Section 106 of the U.S. Copyright Act does not specifically include anything called a "making available" right, the activities involved in making a work available are covered under the exclusive rights of reproduction, distribution, public display and/or public performance set out in Section 106. (*See, e.g., New York Times Co., Inc. v. Tasini*, 533 U.S. 483 (2001), *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993), *Playboy Enters., Inc. v. Webbworld, Inc.*, 991 F. Supp. 543 (N.D. Tex. 1997), *Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distribs.*, 983 F. Supp. 1167 (N.D. Ill. 1997), *Religious Tech. Ctr. v. Netcom On-Line Communication Servs.*, 907 F. Supp. 1361 (N.D. Cal. 1995).) Which of these rights are invoked in any given context will depend on the nature of the "making available" activity.

In the case of a peer to peer network user uploading a copyrighted work onto his or her computer, making it available for other users of the peer to peer network to download, it is simply incorrect to suggest that the person performing the download is the only person legally responsible for infringement. Making the work available in this context constitutes an infringement of the exclusive distribution right, as well of the reproduction right (where the work is uploaded without the authorization of the copyright holder). In the Ninth Circuit's decision in *A&M Records v. Napster*, the court held that "Napster users who upload file names to the search index for others to copy violate plaintiffs' distribution rights." (239 F.3d 1004, 1014 (9th Cir. 2001)).

As you are aware, in implementing the new WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) in the Digital Millennium Copyright Act, Congress determined that it was not necessary to add any additional rights to Section 106 of the Copyright Act in order to implement the "making available" right

under Article 8 of the WCT.[1] Title I of the DMCA was intended to, and did, fully implement the WCT. As I stated in my testimony before the subcommittee, "In our view, [the bill] fully and adequately implements the obligations of the new WIPO treaties, without amending the law in areas where a change is not required for implementation." Since existing U.S. law already covered the activities encompassed in a making available right, "The treaties [did] not require any change in the substance of the copyright rights or exceptions in U.S. law." (H. Rep.105-551 at 15.)

Please let us know if you have any further questions or would like us to provide you with a more detailed analysis.

Sincerely,

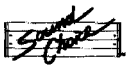
Marybeth Peters / JF

Marybeth Peters
Register of Copyrights

The Honorable Howard L. Berman
Subcommittee on Courts, the Internet and Intellectual Property
B-351A Rayburn House Office Building
Washington, D.C. 20515

[1] Article 8 provides in pertinent part that:

"[A]uthors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including *the making available* to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them." WCT, Article 8 (emphasis added.)



14100 South Lakes Drive
Charlotte, NC 28273

July 24, 2002

TO:

The Honorable Howard L. Berman
Ranking Member
Subcommittee on Courts, the Internet,
And Intellectual Property
2330 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Howard Coble
Chairman
Subcommittee on Courts, the Internet
and Intellectual Property
2468 Rayburn House Office Building
Washington, D.C. 20515

REF: Berman Bill regarding the use of technology to prevent infringement of copyrighted works on peer-to-peer networks.

Sirs:

My name is Tom Turner, and I am writing on behalf of Sound Choice. We are a small Karaoke music production company in Charlotte, North Carolina. Sound Choice is typical of the small company success story – founded by two brothers in 1985, and successfully grown by these two entrepreneurs to a company that currently employees 65 people. Our copyrighted music is the lifeblood of our company.

Sound Choice was an early pioneer in the karaoke music industry, and today we are one of the industry's leaders. In 2001, the karaoke industry had $173.5 million in sales for machines and music. Sound Choice was responsible for over 10% of that sales volume. Currently, however, our business, and the karaoke industry, is threatened by the piracy of our products. Just last week, Sound Choice had the first lay-off in company history. It impacted 5% of our workforce, and there is the potential for additional manpower reductions. Other firms in our industry are taking similar actions.

It would be easy to attribute this to the current economy, but I believe that would be inaccurate. The sales of machines that play karaoke music continues to grow dramatically – while the sales of the music itself continues to decrease. The number of machines sold in 2001 was nearly double the number of machines sold in 2000 – without any significant increase in the sales of music for all of these new machines. The only explanation for that is the piracy of the music itself.

Sound Choice adamantly supports the proposed legislation to permit the holders of copyrights to use technology to protect those copyrights for illegal distribution on peer-to peer networks. Any action that limits the spread of piracy is welcome legislation to us. We also understand that this is difficult legislation, and that there is a need to protect the public from unwarranted intrusion from technology.

704-583-1616
704-583-1871 (fax)
www.soundchoice.com/karaoke/

We will eventually have to address the same issues on subscription networks, and the more centralized networks, such as FTP sites and IRC channels. In our industry, the IRC channels pose the greatest threat – pirates use these channels to make illegal copies for sale, not just for personal use. And we will have to address the issues of conflicts when technology that legitimately protects piracy on a peer-to-peer network, coincidentally blocks it on another non-protected arena, such as an IRC channel. But we also believe in the rights of the consumer, and the responsibility of Congress to protect those rights. This bill would enact legislation that would permit all of us, as artists, businessmen, and consumers, to proceed cautiously.

Again, I would like to repeat our support for this legislation, and any legislation, that protects the rights of copyright holders. Our copyrights are our business. Without protection, we will eventually not be a business.

Tom Turner
General Manager

The Honorable Howard L. Berman
Ranking Member, House Judiciary Subcommitee
On Courts, the Internet and Intellectual Property
2330 Rayburn House Office Building
Washington, D.C.
20515

September 23, 2002

Dear Congressman Berman:

My name is Michael Wood. I am from Ottawa, Canada and my band "CIRCUIT" has just obtained a US recording agreement. A recording agreement is probably the most desired piece of paper any musician can ever hope to obtain. With a recording contract comes hopes and dreams, some being realized by signing the actual contract and others by the results this deal could bring. By signing the recording contract I entered into an agreement that the record label or an acceptable third party would distribute my material around the world. I have not entered into any such agreement with the music traders around the world that they can do this at no charge.

I do not have a million dollars. In fact, I will not have enough money to even live for quite some time and for this I do not fault the record label. They have given me all they can and an opportunity that ninety-nine percent of all bands never get. I find fault in the way the Internet and Peer to Peer (P2P) piracy has crippled the music industry. I am not in Lars Ulrich's (Metallica) position nor that of Dr. Dre. I am a struggling artist that sees my chosen career being significantly damaged by the current state of affairs.

The Internet has great potential for the future; however the manner in which it currently operates is clearly hurting up and coming artists. Below you will find a list of ways the Internet has changed and hurt the music industry over the past five to seven years.

a) The biggest misconception is that the cost of compact discs to manufacture is approximately one dollar. I agree that the actual physical disc is only worth one dollar; however, it is the intellectual and creative property that the disc contains that is very expensive. It is not unreasonable for a record company to budget one million dollars as the cost to launch a new artist. At $14.00 for a brand new compact disc, the record company would then have to sell over 71,000 copies to just break even on the product. The Internet is providing consumers with the product at no charge. Therefore I believe that it is only logical and fair to say that many more than 71,000 copies of the album are being traded. If the record companies do not even break even the artists suffer in all aspects of their career be it "Development", "Tour Support", "Recording Budgets", "Recording Facilities", "Publishing", "Advances", and "Producers." Brand new artists will suffer the most because record labels will not be willing to release second, third and fourth albums. Artists will never again have the same longevity they once enjoyed.

I) New artists typically generate only $1.00 per sale. Using the above example, an artist would have to sell 1,000,000 units prior to seeing any further money from record sales. It makes it extremely difficult, if not impossible, for new artists these days to re-coup the investment that

has been put into them when 2,000,000 pirated versions of their lead single are being downloaded on the Internet, for free!

b) Due to Internet P2P piracy, record labels are taking on a management role for the artists they are signing. After having a discussion with a major US manager, he stated to me, directly, that new artists are now being encouraged to "Joint Venture" with the labels and have the record companies manage their careers. The labels view this as an extra 10-15% that they take from the artists. The problem with this is that when the artists have issues with the label they do not have proper representation to obtain what they need. Outside management has been a staple of the music industry; something that is deeply rooted in music history. Management has always been the key to negotiating on behalf of the artist. How is it possible to negotiate finances, career decisions and so forth when you are a partner with the company that is responsible for the release of your product? Again, this is not a fault to the record label. Everyone is now simply trying to survive.

c) One argument put forward is that the Internet exposes music to a mass audience. This mass audience, in turn, would be more than willing to come and see a live performance of the music. I strongly disagree and feel that the Internet P2P piracy has killed the touring aspect of artists as well.

i) Record labels no longer have the proper amount of funds to provide adequate "Tour Support" to their artists, especially new artists, such as myself.

ii) If the consumer will not pay $14.00 to have a product in their hands they can enjoy for a lifetime, why would they pay $30.00 for a concert ticket? Live shows at the same time are constantly being uploaded on to the Internet.

iii) Artists can no longer afford to tour as a single or duo package. Back in 1992, two bands on the same bill would fill arenas and stadiums all the time. Now, touring festivals are the way of live performance. It now takes 10 of the top new bands to draw the same amount of people that two bands once did. The cost of the festival tickets average around $30.00. Now ten different groups/artists are splitting the revenue of $30.00 rather than just the two groups/artists a decade ago.

d) For years Artists have relied on "Publishing" as their major source of income. There is no doubt that Internet P2P piracy will subsequently cause the record labels to cross-collateralize into the new artists publishing. This problem will only continue to hurt the artists and even potentially force artists to look at other career avenues.

As you can see, the trickle down effect from the Internet and P2P piracy is larger then most people realize. It effects every aspect of the music industry and exponentially decreases the chances of today's new artists making a living at their chosen career choice.

Two possible solutions I would like to propose would be the following:

1) Due to the "Digital Millennium Copyright Act" it states that "someone providing space on

their server, who has no input on the content, isn't liable for copyright infringement."[1] Instead of trying shut down the music sharing sites themselves I believe it would be more beneficial to investigate who is advertising on these sites. The advertisers in turn, are facilitating the illegal downloading of music by injecting capital into companies that offer music downloads at no cost to the consumer. Thus, making the advertiser responsible for copyright infringement and P2P piracy. On the other hand, once music sharing sites start advertising their services, they must be held accountable for their actions as they are aware of the material and the services available on their site. At the very least, all advertisers should be made aware that they are advertising on a website that is used for illegal activity.

2) All major music sharing sites ie: Kazaa and Morpheus would be all moderated, a system already similarly used by Internet Bulletin Board Services. A song that is being submitted for "sharing" would also have to come with that artist's official website. On the artist's site would be the "Official Government Recognized" statement on the music piracy. There would be a "universal statement" saying "yes, you can share our music over the Internet" or "music sharing is a copyright infringement and therefore, we do not authorize the uploading of our material". This would make the music sharing companies responsible for their actions and they then could face prosecution based on the infringements of the **sound recording copyright** ℗.

In conclusion, there is so much that needs to be done to help the music industry and to save it from extinction. I have a terrible feeling that if trends continue as they have been, I will have to seek another form of employment and give up the fundamental right every human being has. It is not just an American dream but the right of every free-willed person on Earth. The right to his dream and to strive for a single goal. The right to take a valid career path and the right to happiness.

The above simply stated points have only scratched the surface of this problem. There is so much more evidence to present before Congress. I would greatly appreciate and be honored to have any opportunity to come to Washington at your convenience and present more evidence as to how this situation s is putting the professional musician out of business.

Sincerely,

Michael Wood
Guitarist - "Circuit"
16 Wynford Avenue
Ottawa, Ontario
Canada
K2G 3Z4
613.829.1410 (Phone)

---

[1] All You Need To Know About The Music Business, Donald S. Passman, Simon & Schuster, ©2000.

Definitions

Development ~ Funds and manpower hours that a record company once invested in an artist to help launch them onto the world stage.

Tour Support ~ Funds that are given to the artist by the record company to help counter the losses historically incurred by touring.

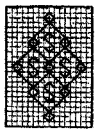
Recording Budgets ~ Funds that are allocated to the recording of an album.

Recording Facilities ~ World class, up to date studios that can put out a competitive product on the world market.

Publishing ~ Separate forms of royalties payable to the artist that are not directly linked to record sales specifically.

Advances ~ Funds given to the artist by record label to help the artist maintain some standard of living.

Producers ~ Person paid by record label to help nurture and develop songs that the artist may have prior to recording them.



Skinner Sisters
PO Box 41786
Los Angeles, CA 90041

(323) 874-5136
facsimile (323) 874-0671
www.skinnersisters.com

finn@skinnersisters.com

Via Facsimile

September 20, 2002

The Hon. Howard L. Berman
Congress of the United States
House of Representatives
Washington, DC 20515-0526

Dear Congressman Berman:

Thank you for your support of creative artists whose intellectual property rights are daily under attack by infringers using the resources available to them on the internet. E-mail, instant messaging, hosted affinity groups and peer-to-peer software services have seriously impacted the needlework industry.

I am an embroidery historian, needlework designer/teacher, needlework publisher and am involved in retail and wholesale sale of my designs and publications. As with many copyright holders in the needlework industry, I am a woman-owned small business requiring other employment to support me.

I have long appreciated the internet and the opportunities it offered to the small business owner. I am able to market my designs to a worldwide audience and offer them for sale on my website. I publish the first (and only) non-commercial needlework e-zine and served as a staff member of a fiber crafts forum on an early online content provider (CompuServe). I own and maintain international online discussion groups for students of needlework and exchange graphics of my work with other designers. Thanks to my ability to scan and transmit my sketches and images of my work-in-progress as well as finished projects I can freely exchange ideas with my colleagues.

Unfortunately, this marvelous technology has created a darkside. We started having difficulties in the needlework industry a little over two years ago when infringers began scanning and uploading copyright protected needlework instructions and designs on photo websites. These infringements included knitting and crochet patterns, embroidery transfers, cross stitch and needlepoint graphs as well as sewing patterns for garment construction and sewing of soft toys and doll clothes.

The infringers soon found they could use free affinity groups hosted by Yahoo, MSN, et al. as hosts to store uploaded infringed designs and distribute them to group members. I joined and maintained membership in over 80 of these groups for more than two years and observed thousands of pages of designs being uploaded.

Those distributing infringed material soon moved on to the use of ICQ, file serve hosting and peer-to-peer group membership. I anticipate they will take advantage of any new file sharing technology available in the future to continue their infringing activities unless curtailed. There exists an entire sub-culture in the needlework industry that is parallel to that in the music industry. The infringers believe it is their "God Given American Right" to scan needlework designs and publications and distribute them to thousands of recipients on the Internet.

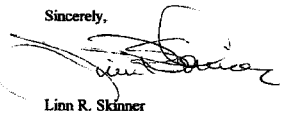
The needlework industry is mostly a woman owned industry, a cottage industry segment of the US economy and our political clout is minimal. We are losing needlework magazines, designers and publishers at an alarming rate. This year our largest industry trade show lost in the range of 25% of its exhibitors. True, not all of our losses can be blamed on Internet pirates, but it certainly is a major factor. I assure you that if one of our needlework publishers brings out a new hardback needlework book, it can be found on the web (in its entirety-100+ pages) within one to two weeks of release. This means a loss of royalties to the designers as well as losses of retail and wholesale sales to the publisher.

In 2001 I felt we needed more than anecdotal documentation of the problem and enlisted a group of volunteers to survey just one Yahoo site where files were being uploaded. We individually examined 35,000 or so messages and found 45,000+ pages of protected material uploaded. We identified, insofar as possible, the publishers and designers of these designs and notified them. We prepared educational materials for our fellow industry members and I have funded the production of the material on a CD for distribution to needlework designers and publishers.

The problem has only grown since then. I stopped monitoring groups in June, 2002 due to a sheer lack of time to do so. Thousands of pages of intellectual property consisting of needlework designs are posted, downloaded or swapped every day and needlework designers seem helpless to deal with the issues. Holders of copyrights need to be able to identify and pursue infringers and/or remove infringed materials. Our only products are our creative designs and when these designs are stolen and distributed without permission of or compensation to the designer, we are seriously impacted.

I applaud your efforts on behalf of those of us who are very much "small business" and not industry titans. The problem of internet piracy affects every creative artist whose art can be distributed via a graphic, audio or video file. As I speak on this issue I hear from photographers, architects, authors, graphic designers, artists, dramatists and others who are struggling with online infringement. Any legislation aimed at the containment of internet piracy will benefit these rights holders and not only the large multi-national corporations of the entertainment industry.

Sincerely,



Linn R. Skinner

The Heritage Foundation
Executive Memorandum

214 Massachusetts Avenue, N.E., Washington, D.C. 20002-4999 • (202) 546-4400 • http://www.heritage.org

No. 835 September 25, 2002

SELF-DEFENSE: A DIFFERENT TUNE ON COPYRIGHT

JAMES L. GATTUSO AND NORBERT J. MICHEL

As the Internet has grown, music companies, Hollywood filmmakers, and other copyright owners have watched in horror as digital technologies have made it increasingly easy to copy and distribute their property without payment. All too often, the response of these copyright owners has been to lobby for potentially harmful regulation of new technologies and overly protective copyrights. This summer, Representative Howard Berman (R–CA) proposed a radically different approach: allowing copyright owners to use digital self-help measures to protect their own intellectual property.

The proposed legislation (H.R. 5211) has been met with a firestorm of controversy. Critics have assailed the prospect of "posses of copyright vigilantes" and music company hackers deleting hard drives. In reality, the Berman bill is narrowly drawn, allowing copyright holders only limited actions and including legal penalties should they go too far. Most important, while reasonable people could disagree about the specific language, the concept of self-help is both sound and a welcome alternative to government regulatory intervention in this vital field.

The Peer-to-Peer Explosion. The underlying controversy here is a practice known as "file sharing." Pioneered by Napster in 1999, file sharing initially enabled users to "share" digital copies of songs after being placed on a central computer.

Because file sharing enables widespread distribution of copyrighted material—without payment of royalties to the creators—Napster's activities were ruled illegal in 2000. File sharing continues, however, through more decentralized "peer-to-peer" (P2P) networks. These networks allow users to share files by plugging in directly to other users' computers. This decentralization makes it more difficult to pursue copyright violators in court, as was done with Napster.

Moreover, these networks are not just technical toys used only by a few committed techies. KazaA, one of the most popular networks, boasts that its program has been downloaded over 100 million times. According to KazaA's Web site, some 2 million people are using it at any one time. In addition to losses to intellectual property owners, Internet users themselves could be hurt by such widespread, unauthorized distribution—as producers are discouraged from providing content for new digital services.

Produced by the
Thomas A. Roe Institute for
Economic Policy Studies

Published by
The Heritage Foundation
214 Massachusetts Ave., NE
Washington, D.C.
20002–4999
(202) 546-4400
http://www.heritage.org

This paper, in its entirety, can be found at: *www.heritage.org/research/regulation/em835.cfm*

No. 835 Executive Memorandum September 25, 2002

Long Tradition of Self-Help. Congressman Berman's proposal would make it easier for copyright owners to employ self-help measures to defend their products against such networks. The general concept of self-help against theft is nothing new to the law. Homeowners, for instance, have long been able take reasonable action to stop burglars found in their homes, and storekeepers are entitled to stop shoplifters. Moreover, it is common for lenders to repossess automobiles and other secured items. The owner's consent is not needed, and lenders are explicitly allowed to enter the debtor's private property in order to repossess. The right of property owners to act is far from unlimited—for instance, homeowners may not simply shoot burglars on sight—but within clear limits, self-help is widely accepted.

The property at issue here—musical recordings and movies—is intangible intellectual property, but the principle remains the same. If, under the relevant copyright laws, these goods are being distributed without the owner's consent, the owner should be allowed to impede the theft.

Specifically, the Berman bill protects owners from liability for "blocking, diverting or otherwise impairing the unauthorized distribution…of his or her copyrighted work on a publicly accessible peer-to-peer file trading network." Copyright owners, however, would not be able to "alter, delete, or otherwise impair the integrity of any computer file or data residing on the computer of a file trader." The owner would also have to inform the Department of Justice in advance of any action to be taken.

Given the rapid pace at which technology changes, the bill, appropriately, does not list specific actions that would be allowed. Among the most likely to be used, however, is "spoofing"—flooding the P2P network with an enormous number of flawed or altered copies of the copyrighted material. For instance, to disrupt the distribution of the movie *Spiderman*, Sony might create 10,000 alternate files that appear to be *Spiderman* but actually are something else, such as static. Alternatively, a technique known as "first-in-line interdiction" could be used, by which a copyright owner would download certain materials from the P2P network at extremely low speeds, thus making them unavailable for others.

Boundaries of Self-Help. Equally important are the actions that H.R. 5211 would *not* allow. Files could not be deleted or corrupted. Indiscriminate "denial of service" attacks—shutting down P2P networks entirely—would not be allowed, since this would impair the legitimate activities of the network.

H.R. 5211 also allows P2P traders to sue if copyright owners go too far. Most important, if copyright owners should go beyond what H.R. 5211 permits, individuals are explicitly allowed to file suit for violations under any *existing* laws and can recover any damages those laws allow.

Moreover, the legislation creates a new legal claim, "wrongful impairment." While this process is limited—the Attorney General, for instance, can keep such claims from going to court—it only supplements, rather than replaces, current mechanisms for redress. As a final check, H.R. 5211 allows the government to prevent a copyright owner from using any self-help measures if it finds a pattern of abuse.

Congressman Berman's proposal is not perfect. Critics have pointed out that some provisions are ambiguous. For instance, it allows copyright owners to impair the availability of non-infringing computer files to the extent "reasonably necessary" to prevent unauthorized distribution of a protected work. But what is "reasonable?" At worst, this is a potential loophole in the protections given to computer users; at best, the term invites litigation. Such ambiguities should be cleared up as the bill progresses.

Adapting intellectual property rules to the reality of today's digital age will be no easy task. This Gordian knot has no simple solution: It entails forging a delicate balance between the rights of content owners and users without hobbling technological innovation. Representative Berman's proposal, while not a cure-all, could be one small step in the right direction.

—James L. Gattuso is Research Fellow in Regulatory Policy in the Thomas A. Roe Institute for Economic Policy Studies, and Norbert J. Michel is a Policy Analyst in the Center for Data Analysis, at The Heritage Foundation.

N S A I

September 24, 2002

The Honorable Howard L. Berman
2330 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressman Berman:

The Nashville Songwriters Association International continues to appreciate your ongoing efforts to offer songwriters and other legal copyright holders tools to combat the illegal distribution of their property. We need every tool available to fight peer-to-peer piracy.

If someone is stealing a song on a peer-to-peer network, the creator of that song has every right to block its distribution. It is the songwriter's property in every sense of the word. The key word is "permission." No one should be able to distribute or utilize someone else's property without their permission.

Songwriters greatly depend upon royalties to pay rent, buy groceries, and pay for childcare along with other day-to-day living expenses. Very few songwriters are able to live on royalties alone.

NSAI and its songwriter members thank you for attempting to provide technical solutions to allow songwriters to combat the theft of their property.

Sincerely,

Barton Herbison, Executive Director
Nashville Songwriters Association International

Nashville Songwriters Association International
1701 West End Ave., Third Floor • Nashville, Tennessee 37203 • Phone (615) 256-3354
Fax (615) [illegible]-2034 • Website: www.NashvilleSongwriters.com • E-mail: nsai@NashvilleSongwriters.com

The Songwriters Guild of America

Serving The American Songwriter For Over 70 Years

1500 Harbor Blvd.
Weehawken, NJ 07086-6732
TEL: (201) 867-7603
FAX: (201) 867-7535
LBachman@aol.com
http://www.songwriters.org

Lewis M. Bachman
Executive Director

July 16, 2002

BY HAND

Honorable Howard Berman
2330 Rayburn House Office Building
Washington, DC 20515

Dear Congressman Berman:

On behalf of the 5000 members of The Songwriters Guild of America (SGA), I am writing to strongly endorse the concept of your proposed "peer-to-peer" piracy legislation to be introduced later this week. SGA is immensely gratified that you are once again at the forefront of the effort to protect our creations -- and our livelihoods -- from the scourge of rampant piracy.

As you well know, SGA is the nation's oldest and largest organization run exclusively by and for songwriters. The Guild provides contract advice, royalty collection and audit services, copyright renewal and termination filings, and numerous other benefits to our members. In addition, SGA and its Songwriters Guild Foundation help beginning songwriters through scholarships, grants and specialized Guild programs. We have offices in New Jersey / New York, Nashville, and your home city of Los Angeles.

In your July 9 statement on CNET announcing your proposal for peer-to-peer legislation, you made crystal clear the toll that piracy is taking on songwriters. As you said, each illegal download of a musical composition robs the creator of the eight cents due under the statutory mechanical license, a key component of a writer's income. As you also pointed out, *one* peer-to-peer system alone can lead to well over one billion downloads *in a single month*, which means nearly $100 million a month in royalties may be lost through a single network. As you said: "Divide even one-tenth of that money among the 5,000 members of The Songwriters Guild of America, and you begin to see that P2P piracy robs songwriters on a massive scale."

Even prior to the advent of the digital revolution, songwriting was an extremely difficult occupation, with a high likelihood of failure and only a slight chance of real success. It has been estimated that less than ten percent of songwriters are able to earn a living solely from creating music. Given their already precarious lives as creators, songwriters simply cannot continue to sustain the grievous financial losses caused by the

worldwide piracy epidemic. Guild members may, as you have said, write because they love music, but they cannot live on love alone.

Your legislation would help mitigate the intolerable piracy situation by providing songwriters and other copyright owners with the ability to use technological tools to prevent theft without risking potential liability under state or federal law. At the same time, your bill is carefully balanced; it aims to protect peer-to-peer users as well as copyright owners. For example, your bill does not allow the removal of files from, or the corruption of files on, a peer-to-peer user's computer.

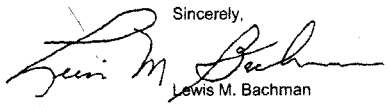
The staggering scope of peer-to-peer piracy is a direct threat to the American music industry, one of the crown jewels of our nation's economy. It is a particular menace to songwriters, on whose efforts the entire industry depends. Unfortunately, current law provides us with virtually no options for addressing this problem. Prosecution of individual copyright infringement cases is fraught with legal problems and is not economically or politically feasible.

We desperately need a variety of new approaches as part of an overall effort to curb peer-to-peer piracy. By giving songwriters and other copyright owners the ability to use technological self-help in stemming the theft of our creations, your legislation represents an important next step in responding to the piracy problem.

SGA emphatically urges prompt consideration of your peer-to-peer piracy legislation. And we join with all our colleague creators in thanking you once again for your long-time, dedicated efforts to protect intellectual property

With warm regards.

Sincerely,



Lewis M. Bachman

P2P Fear and Loathing: Operational Hazards of File Trading Networks

John Hale, Nicholas Davis, James Arrowood and Gavin Manes

Center for Information Security, University of Tulsa

***Abstract*—Peer-to-peer (P2P) networking technology has revolutionized file sharing over the Internet. Proprietary and open source P2P ventures alike have taken flight, facilitating public file sharing on an unprecedented level. Unfortunately, careful investigation of P2P security and digital rights management issues has not followed hand-in-hand with wide-spread acceptance and use of the technology. P2P networking clients expose systems to a variety of security and privacy hazards. Moreover, rampant copyright infringement over P2P networks has spurred the development of electronic countermeasures to thwart would-be infringers. This paper examines the security and privacy risks associated with P2P networks, as well as electronic countermeasures to copyright infringement over P2P networks.**

***Index Terms*— blocking, digital rights management, electronic countermeasures, file sharing, interdiction, network security, peer-to-peer networks, redirection, spoofing, viruses, worms.**

I. Introduction

Peer-to-peer (P2P) networking technology has revolutionized file sharing over the Internet [2, 3, 4, 7]. Proprietary and open source P2P ventures alike have taken flight, facilitating public file sharing on an unprecedented level. Unfortunately, investigation of P2P security and digital rights management issues has not followed hand-in-hand with wide-spread acceptance and use of the technology.

P2P networking clients expose systems to a variety of security and privacy hazards. Systems running P2P networking clients may be vulnerable to software design and implementation flaws that provide an open door for hackers. What distinguishes this threat from that posed by flaws in other applications is that the heightened connectivity of systems running P2P clients greatly increases the level of exposure, and accordingly the risk of operation. Privacy concerns related to the potential for (and in some cases documented existence of) spyware embedded in P2P clients also have not diminished.

Moreover, the most popular P2P networks have become a breeding ground for copyright violations of all digital media – copyrighted music, movies, software and games are openly traded. Where cryptography has failed to provide a solution, rampant copyright infringement over P2P networks has spurred the development of alternative electronic countermeasures to thwart would-be infringers. This paper examines security and privacy risks associated with P2P networks, as well as electronic countermeasures to copyright infringement over P2P networks.

II. Peer-to-Peer Trading Networks

File sharing networks based on peer-to-peer technology typically embrace one of two server models; centralized or decentralized. The difference to users is transparent, but can have subtle implications for system security and for electronic countermeasures. This section briefly describes each model.

A. Centralized P2P Model

Napster popularized the centralized P2P model, and demonstrated the viability and power of a simple network overlay architecture on the Internet [2]. The Napster P2P model relies on a centralized server (or a collection of servers) to maintain an index of downloadable files on participating network clients (Figure 1).

To participate in this kind of a P2P network, a user must download and launch a software client. The client registers itself in the network by communicating to the server and listing the files available for download, which are located in a designated shared folder. The client also sends connection information to the server; its IP address, purported connection type (e.g., T3, T1, Cable, DSL or dial-up), and other metadata. Clients periodically send updates to the server to ensure a current index.

Keyword-based queries (Figure 1 - Q) for files are issued from a client to the server, which then reports back to the requesting client any hits (Figure 1 - H), identifying the location of all clients that have files matching the search criteria. A download request is then made from the originating client directly to the client hosting a desired file, and the download process begins (Figure 1 - D). Commonly, the download process is accomplished via a separate network protocol, e.g., HTTP – the protocol used to download web pages from sites across the Internet.

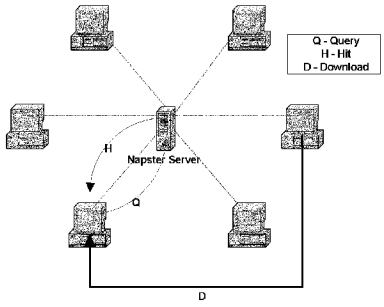


Figure 1: Centralized P2P Model.

The primary performance issue in the centralized model is that the server, since it must index every host and respond to every query, is a potential bottleneck. However, server replication is a simple and effective strategy for overcoming this obstacle, allowing P2P networks to scale in number of participating hosts. The tradeoff for this scheme is added complexity of server-to-server communication and logic for index integrity and consistency.

B. Decentralized P2P Model

The decentralized architecture features a purer implementation of the peer-to-peer networking philosophy (Figure 2). Gnutella and other decentralized P2P schemes rely on each client to support query/response functionality [3]. The only server-like systems involved in these networks are those nodes that help clients bootstrap themselves into the network by providing them with a list of peer node IP addresses in the client's neighborhood.

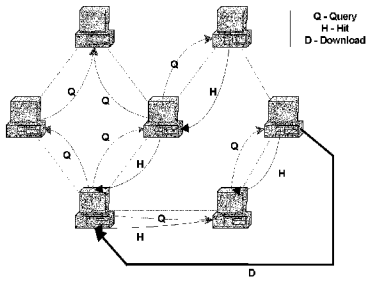


Figure 2: Decentralized P2P Model.

Once again, participation requires the installation of client software to launch the bootstrap process and issue and respond to queries. The collection of network nodes visible to a given client defines its horizon. The horizon for a node is dynamic and is directly related to timely network replies compared against Time-To-Live (TTL) parameters, which establish the lifetime (typically by hops) of query messages originating from a client.

In decentralized P2P networks, file queries (Figure 2 - Q) are issued from a client directly to other nodes in the client's horizon. Clients receiving queries may respond directly with a hit message (Figure 1 - H), or pass the query along to other nodes in its horizon. One subtle feature in the most common decentralized model implementation is that hit response messages traverse back through the original query path, as opposed to flowing 'directly' back to the query host from the responder. Download requests are made from the querying client directly to the client reporting the hit. (Figure 1 - D). Again, it is common practice for the actual download process to occur via a separate network protocol, such as HTTP.

III. P2P Network Threats

Most P2P networks share characteristics that increase the risk of operation for participating systems. Extreme and anonymous connectivity inherent in P2P networks creates an environment in which establishing and maintaining core security properties of integrity and non-repudiation is a difficult, if not impossible, task. P2P file traders run a higher risk of machine crashes, loss of privacy, even having their systems commandeered by hackers. Threats to P2P users may not only come from hackers lurking in dark corners of the network, but also from the client software itself. This section examines the dangers posed to P2P networks by spyware, trojan horses, system exploits, denial of service attacks, and worms and viruses.

A. Spyware

The most prevalent threat to user privacy in P2P networks is spyware. Spyware takes many forms; from annoying software that sends registration form data to third parties for consumer profiling, to more insidious programs that track user activity and steal sensitive information off of hard drives.

Developers routinely bundle spyware and adware with P2P clients as a way to generate a revenue stream from their freely downloadable software. In P2P networks, spyware complements adware by monitoring user behavior and constructing user profiles from various data sources on a user's system. In particular, P2P spyware tracks user browsing habits to facilitate target-marketing campaigns that often incorporate adware (pop-up and banner advertisements). In addition, registration data is regularly sold to direct marketing firms.

While there is no indication that this practice will diminish, "clean" versions of P2P clients (purportedly without spyware) have surfaced [5]. Even so, no foolproof method of checking for the absence of spyware in these (or any other) applications exists.

B. Trojan Horses

Trojan horses are executable code embedded in system or application software with unexpected and possibly malicious behavior. They may leak information, corrupt files, or allow an intruder to gain unfettered access to a system. The wide install base and lax security of personal computers running P2P clients makes them attractive targets for trojan horses.

However, the primary threat comes not from the core client itself, but from the collection of software and adware bundled with the client. In January 2002, Symantec classified a P2P client spyware program called "W32.DIDer" as a trojan horse because, even after users opted to block installation of the carrier code, it installed itself on users' systems [1]. The offending code was bundled in clients for four separate P2P networks. At the time, one of the P2P networks involved boasted a client install base of over 1.3 million systems.

C. System Exploits

System exploits take advantage of application-level vulnerabilities due to flaws in software. Exploits are often captured in scripts and posted on hacker websites that any novice can access. They can be designed to achieve a number of malicious objectives.

By far, the most common form of software system exploit is the buffer overflow attack. Buffer overflows capitalize on weak bounds checking of parameters to overwrite strategic regions of memory. In some cases, overflowing a parameter or variable may have no discernable effect. On the other hand, it may crash a system. In a skilled buffer overflow attack, executable code is written into memory and run, potentially giving a hacker full control over a host. Other kinds of system exploits, such as race conditions and trust abuse occur less frequently, but can yield similar results.

As in any program, P2P client software is susceptible to design and implementation flaws. Unfortunately, the open nature of P2P clients makes buffer overflow and other system exploits more likely, and potentially more devastating. P2P clients must, by definition, expose network service interfaces and other functions that can easily be probed for flaws and weaknesses by hackers. For example, an alleged cross-site scripting vulnerability was reportedly found in some early Gnutella clients and is currently under review [6]. The weakness allows attackers to execute arbitrary code on remote systems. Unfortunately, the increasing richness of P2P client service features and functions correspondingly increases the potential number of latent software vulnerabilities, which can lay dormant for years until they are discovered by a hacker.

D. Denial of Service Attacks

Denial of Service (DoS) attacks are among the most potent weapons in a hacker's arsenal. They are also the most challenging to contend with. DoS attacks can happen at any level of a network and/or application. Some DoS attacks may consist of malformed packets designed to crash systems. Others may rely on network traffic floods to take down a system or router, even engaging multiple hosts to force-multiply the impact of the attack; the most extreme of these enslave a legion of hosts in order to launch a massive wave of packets at a target in a Distributed Denial of Service (DDoS) attack. Such attacks can encumber substantial collateral damage; while the intended target may be a host, an entire network could be equally impacted.

In as much as DoS attacks degrade performance or disrupt service for networks and systems, they likewise impact P2P users and networks. However, it is possible that certain types of DoS attacks may target hosts, or even specific applications on hosts, leaving other system elements relatively unharmed. For example, jamming the upload queue of a P2P client with a flood of download requests may effectively block other users from accessing files on that host, but have no other substantial impact on the host itself or the network to which it is connected.

E. Worms and Viruses

Worms and viruses have as much potential to overwhelm computers and networks as do DoS attacks. Both infect hosts via system exploit and/or social engineering, cover their tracks, and reproduce to move across a network. Worms propagate without human intervention, using network services and communication channels to spread. Viruses rely on humans to move from system to system. The payload in viruses and worms may be malicious or benign, but in either case the massive reproduction of self-replicating code may be enough to cripple hosts or regions of a network.

A recent spate of virus attacks has inflicted damage on popular P2P networks [8]. One of the earliest, the "Benjamin" virus, propagates itself across the Kazaa P2P network through a combination of social engineering and localized replication in share folders. The virus relies on a user download to move from machine to machine across the Internet. Once the code is activated, the virus copies itself to a shared directory under a variety of names and displays a website containing banner advertisements.

Even though these P2P viruses need humans to download them to spread, it is not difficult to envision a true P2P worm that replicates itself throughout shared folders by using vulnerable client communication channels. Such a worm might infect a host by identifying and exploiting a latent buffer overflow exposure residing in client network service functions. Copying its own code into the communication buffer, it would not rely on human interaction to propagate, and therefore could spread much faster.

IV. P2P Digital Rights Management

As researchers seek elusive cryptographic solutions to the digital rights management problem, a collection of electronic countermeasures have been developed that strike at digital piracy distribution models. Blocking, interdiction, spoofing and redirection all aim to inhibit the trading of copyrighted media in P2P file sharing environments. It is important to note the schemes described in this section do not engage "hacking" techniques to foil digital media piracy. Each technique has its relative merits and disadvantages, but collectively, they represent the only practical technological means of dealing with copyright infringement over P2P networks.

A. Blocking

The most straightforward technique for inhibiting illegal file trading in P2P environments is to block queries and/or hit response messages as they try to move across a network (Figure 3). This can be accomplished with a simple firewall or router by blocking the appropriate ports used by communicating P2P clients. The net effect of this approach is that regions of P2P networks are isolated from the rest of the network, unable to communicate or trade files. Successful implementation of this strategy requires control of some region of the network, and thus is ideally suited for enterprises and Internet Service Providers (ISPs). (While blocking helps some private enterprises cut down on digital piracy and curb bandwidth consumption, public ISPs appear more than reluctant to adopt this approach.) Depending on the implementation, a blocking solution may restrict P2P communications for an entire enterprise network, a subnet or collection of subnets, or an individual host.

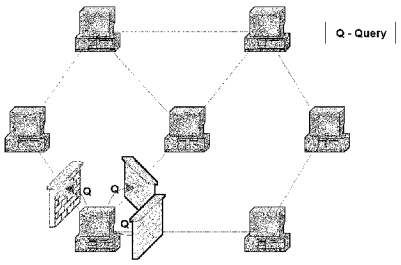


Figure 3: Blocking.

The drawbacks to this approach are significant. Blocking solutions typically cannot discriminate between illegal file trading and legitimate queries and downloads. Moreover, depending on the load of the network, the blocking hardware, the countermeasure may constitute a bottleneck. Lastly, simple port-hopping and tunneling strategies are effective ways to elude network blocking and filtering devices, making it more difficult to locate and disrupt copyright infringing downloads and communications.

B. Interdiction

Interdiction constitutes a high-level Denial of Service attack on P2P client download functions (Figure 4). The objective of this countermeasure is to swamp the download request queue of a copyright infringer with requests so that no illegal copyrighted media can be downloaded from the infringer's system by third parties. Implementation engages an array of hosts – interdiction servers – dedicated to locating infringers and issuing a stream of download requests to keep their queues filled over time.

This approach differs from low-level DoS attacks in that it surgically strikes at an application-level weakness – the limited capacity of the P2P client download request queue. Whereas a conventional DoS flooding attack may direct thousands of messages at a target instantaneously, a slow but steady stream of download requests will likely suffice to greatly diminish an infringer's ability to share files over a P2P network. The principal drawback of this approach is that requests for legitimate media to the infringer's host are affected as well. In addition, smart clients may be programmed to ignore repeated download attempts from the same client in an attempt to circumvent the countermeasure.

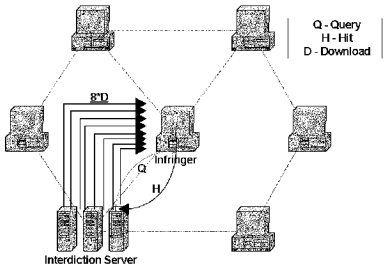


Figure 4: Interdiction.

C. Spoofing

Like interdiction, spoofing countermeasures aim to prevent digital media copyright infringement by overwhelming P2P networks (Figure 5). However, while interdiction attacks the download process, spoofing targets the search process. This technique floods P2P indexes with decoy metadata in a centralized architecture, e.g., Napster networks, and responds to queries for copyrighted media with bogus responses in a decentralized architecture, e.g., Gnutella networks. The intended effect of spoofing is to make locating authentic files in a trading network nearly impossible by ensuring that decoy hits drastically outnumber legitimate ones.

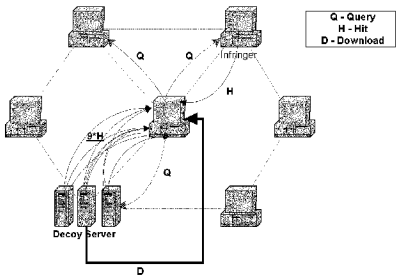


Figure 5: Spoofing.

Spoofing typically requires an array of systems serving up decoy information. The bandwidth economics of spoofing is more attractive than interdiction because the process yields a flood of media metadata, substantially less expensive than the constant stream of downloads incurred by queue jamming. Moreover, spoofing does not inhibit legitimate file trading by anyone, it targets the media, not the infringer.

Decoy media manufacture and download strategies play a key role in the success of spoofing schemes. Decoy media must appear authentic in all ways to requesting clients – in size, name, format, and all other media characteristics visible to users in P2P search engines. The download process can be metered to preserve network bandwidth. Download preview functions also pose a challenge to manufacturing decoys, but techniques have been proposed to construct decoy media files that appear authentic in their initial seconds of play. This minimizes the effectiveness of preview functions as decoy filters.

D. Redirection

Redirection perpetrates a bait and switch on users looking for copyrighted digital media in file trading networks (Figure 6). In Gnutella-style networks it exploits the messaging protocol, which mandates that the response path follow the query path for media searches. Intermediate hosts along the query path falsify and corrupt response messages (Figure 6 – H1) so that subsequent download requests (Figure 6 – D5) are misdirected. Strictly speaking, redirection in Napster networks is not possible without penetrating the server index core services.

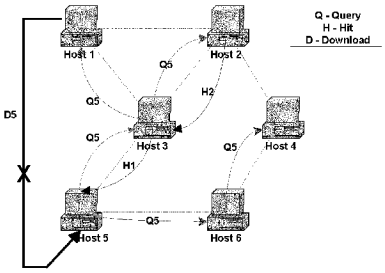


Figure 6: Redirection.

This approach has an ultimate effect similar to that of spoofing, except that its "decoys" actually replace some infringer search results. Would-be infringers even can be redirected to alternative content. However, a simple modification to the P2P messaging protocol permitting direct query responses (as opposed to responses that follow the query path) would eliminate the opportunity for intervening clients to alter or forge response messages.

V. Conclusions

Users and adopters of peer-to-peer technology must understand associated operational hazards, including inherent security vulnerabilities and exposures, as well as implications of imminent P2P digital rights management strategies. Next generation P2P networks promise greater anonymity, more powerful search engines, and anticipate an underlying Internet infrastructure that delivers broadband connectivity to virtually every desktop. Unless security architectures and electronic countermeasures for network media piracy keep pace with P2P technology, developers, network administrators and users alike will find increasing operational risk and greater digital media copyright protection challenges in the future.

References

[1] Borland, J., *File Sharing Programs Contain Trojan Horse*, Tech News – Cnet.com, http://www.cnet.com , January 2, 2002.

[2] Dr. Scholl (pseudonym), *OpenNap Napster Protocol*, http://opennap.sourceforge.net, 2000.

[3] LimeGroup, LLC. *The Gnutella Protocol Specification v0.4.*, http://www2.limewire.com.

[4] Cho, S., Understanding Peer-to-Peer Networking and File-Sharing, http://www.limewire.com: , 2002.

[5] Menta, R., *Clean LimeWire - All the flavor without all the SpyWare*, MP3 Newswire.Net http://www.mp3newswire.net, January. 10. 2002.

[6] MITRE, Common Vulnerabilities and Exposures Database, CAN-2001-1004, http://cve.mitre.org, August, 2001.

[7] Singh, M., Peering at Peer-to-Peer Computing. *IEEE Internet Computing*, **5(1):** 4-5, 2001.

[8] Vamosi, R., *The Rise of P2P Worms*, ZDNet, http://www.zdnet.com, September. 18, 2002.

PREPARED STATEMENT OF STEPHEN HINKLE

I bring this testimony to the aid of three file sharing services, and their parent companies, MusicCity, KaZaa, and Grokster.

My name is Stephen Hinkle, and I currently work as a Network Tech for the City Heights Educational Pilot. The CHEP is an educational program in City Heights that works with some inner-city schools. I am also a computer science student at San Diego State University.

I have been following this "internet music crisis" for a couple of years now. Every since the Recording Industry Association of America (RIAA) sued Napster, I was interested in following it. I have then written several articles for Boycott-RIAA.com, a site about the "bad acts" of the music industry and their effect on artists and consumers.

As a consumer, a student, and a representative for the educational community, I have deep concerns that the RIAA, MPAA, and NMPA collaborating to try to shut down file sharing services will hurt the economy, emerging artists, consumers "fair use rights", and will hinder music distribution in cyberspace.

History of File Sharing Cases:

The RIAA first sued Napster, then Scour, then Aimster [now called Madster], and now MusicCity, KaZaa, and Grokster, and finally AudioGalaxy. In my opinion, the intent of these lawsuits was to *bankrupt* the file sharing companies, not to ever be "fairly tried" by jury.

For example, the plaintiffs in the AudioGalaxy case asked for over 100 million in damages. In the Scour case, the stakes were much higher, at 250 Billion. It seems like very few, if any business could pay such exorbitant amounts. Some of the people who operated the services got *sued personally*, which means that their own family could be in debt for life.

In my opinion, and others I talked to, and from articles I have read, I believe that file sharing has substantial non-infringing uses, allows consumer "fair use", and can be an excellent content distribution medium.

How File Sharing is good for Content Creators:

Many musicians claim that file sharing actually helps them in music business. Many indie and major label artists think that file sharing is actually good, because it gives people a chance to hear their music, who would not hear it on the radio. Artists from BB King, Courtney Love, Janis Ian, Dave Matthews Band, Lara Lavi, The Rosenbergs, and many others say that "file sharing" has helped promote them, including sharing on the Morpheus, KaZaa, and Grokster networks.

Major and independent label musicians have a lot to gain from P2P sharing, even if it is not financially. Many people that I talked to told me that they have bought more CDs as the result of getting to hear what they are buying first.

A lot of bands want to use MP3 downloads for promotion, but the labels do not allow them to on their own web sites, and many have to turn to file sharing networks to do so. This is because the labels often make the artists sign their rights away. I know a lot of unsigned bands are beginning to use P2P companies to get their music known. The best-known program was *Napster's New Artist Program*, before Napster went under. Now, others have taken over this task, including *Streamcast Networks*, by featuring new artists on their *Morpheus* service. Another example is Grokster's partnership with GigAmerica, which features unsigned bands. Centerspan also allows unknown bands to be featured on their Scour service, as well as Universal's Emusic.

In addition to music, there are other good uses for P2P. *Reelmind*, the independent film organization, partnered with Grokster to promote its films on the Grokster P2P network. Other uses include photographs, cooking recipes, and efficient distribution of public domain or open source software.

Consumer's common uses of P2P:

The number one use of P2P by most consumers is to download media files (music, video, etc), and to Discover New Music. Most consumers like a much bigger variety of media, than just what the RIAA and MPAA want people to hear or see. I have talked to many people on their uses of P2P, below are common things I have heard from them.

In these days of high costs of living, many consumers are budget-savvy, and want to decide if something is worth buying. Many people, especially college students do not have too much money to waste on "bad CDs", or CDs that are not worth their money. So, they download a few songs off the CD, to see if it is worth their money. Many adults end up buying more CDs, by sampling first.

The next common P2P use by consumers is to download songs they already own because it is easier to download a song, than it is to "rip" it for their CD. This should be a "fair use", since the consumer already owns the material. Many people do this for their computers in another room, at their office, or for their portable digital music players (often called MP3 Players, since MP3 is the most common format for compressed digital music).

For many consumers who burn Audio CDs, they do not burn entire albums downloaded from P2P systems. Instead, they burn "custom collections". A custom collection is a selection of songs from many different artists or albums on the same CD. For example, if one wanted one song by Alicia Keys, another by Bob Dylan, another by Dixie Chicks, another by Mandy Moore, on the same CD, it would be a "custom collection".

The next reason that people use P2P is to obtain music, movies, or other content that is no longer sold in stores. For example, my mom could not find "White Bird" by "It's a Beautiful Day", and she remembers it from her childhood. However, I punched it into Napster, and it was there! Many people use P2P for this, is because more than 60% of the music catalog of the labels is not sold at any given time. In my opinion, there is no cost to anyone, if the song or other content is no longer available anywhere else.

For most video P2P users, they download TV shows they missed, or movies that they want to see if it is worth paying the high price of movie tickets for. Since the price of a movie ticket in San Diego (where I live), is about $9.00 per person, an that does not include Popcorn, Drinks, or other stuff you get at the movies, it is worth using P2P to "sample a movie" before you go see it. People will download clips of movies, or even an entire movie from a P2P service to see it is worth seeing on the big screen.

Most video files are huge (between 650MB and 3GB for a two-hour film), and downloading one can take a lot of time (over 6 Hours on a Cable Modem), especially if the other P2P user has a slow uplink (most cable and DSL connections uplink much slower than they downlink). Since the space is so large, many users delete them shortly after they are played. Even if they get burned to CD for permanent storage, the quality is usually nowhere near broadcast or cinema.

For other content, some people said they download Software, books, and the like. Many users who do this are low income, and many people told me that they would buy a copy, if they could do so. Also, many people download "free" software, which is software licensed for open source distribution. Linux is one example of this.

Consumer reactions to legal actions against P2P:

Many consumers were upset when P2P companies such as Napster and Scour got sued. Many consumers loved the fact that they could get easy access to a vast library of media. The selection offered was better than any record or video store on the planet. When the injunction that ordered Napster to be shut down, consumers began to hate the music industry, and when the artists came out on how their labels cheated them out of being paid from their CDs, people no longer wanted to support the industry's side.

When the RIAA started threatening college campuses to block access to P2P in their dormitories, it made many college kids upset. In response to these attacks, P2P developers worked to make their network harder to block or shut down. Also, it made a lot of college kids not want to buy the CDs of the company that did this. At San Diego State University, who instituted the blocking with *Packeteer* (a company who markets filtering for P2P sharing), now use all sorts of tricks to get around the block, such as running Gnutella clients, and share within the dorm network, and use hard to block programs P2P like Filetopia 3.0 (which combines Random Ports, Decentralization, and High-Bit Encryption).

Many consumers now feel that their data is at risk, with the event of the *Howard Berman Bill*, which would legalize some P2P hacking attacks, and Denial-of-Service attacks against consumers. Many tech-savvy consumers say that this is taking things too far. The Electronic Frontier Foundation, Boycott-RIAA.com, and DigitalConsumer.org, report that consumers' privacy is at risk, as well as their constitutional rights. I believe this too, and that is one reason I am writing this testimony. This prompted *Information Wave Technologies* to block the RIAA and its "hired spies" from accessing its network.

With the P2P lawsuits, consumers and artists alike began to question the music industries practices of greed, and many of them are getting heavily exposed. Many consumers and artists are appalled that artists can sell millions of records and make nothing off of them. As such, coalitions such as the Recording Artists Coalition, Digital Consumer, Future of Music, and others were formed.

Consumers are upset and more concerned, by the music and movie industries trying to mandate Digital Rights Management technology (DRM) in almost every electronic device. This would seriously limit what ways that one could use a computer, and even give them "unfair competition" because their definition of "unauthorized" would include everything not owned by their oligopoly. Independent musicians, software writers, filmmakers, and the like should be able to distribute content in unprotected format if they choose. Licenses like the GNU General Public License, the Open Audio License, and others are designed to specifically allow distribution.

The proposed CBDPTA bill, that Senator Fritz Hollings wrote would ban even e-mailing a friend a word document, or being able to turn in a program you created for a programming class. As a member of the academic community, with the use of distance education becoming more common, this bill would kill it. Consumers are upset that the RIAA and MPAAs attempt to ban a technology, just because it could be used for infringing copies. History has shown that every technology the entertainment industry has been afraid of has benefited them. This has been true with tapes, CDs, VCRs, MP3 Players, DAT Recorders, and the like.

Many consumers are worried that the industry is lobbying to take away the rights to copy ANY digital medium, and that the industry is taking their "fair use" rights away. Fair use rights include "space shifting" (to move data from one medium to another, or to another room in their home, or to their car, etc), "time shifting" (to record a broadcast and play it back later), "quoting" (to use a small sample for speech or academic projects), and "reverse engineering" (to figure out how a device works, to make something compatible with a device or format (such as emulation or interoperability).

The entertainment industry has sued literally every device maker, claiming that every new feature is "copyright infringement", and some under the Digital Millennium Copyright Act (DMCA). For example, the RIAA tried to stop the sale of MP3 players. The MPAA are trying to stop the sale of ReplayTV recorders because they can send shows to other units, and skip commercials. The same happened with DeCSS and the Advanced E-Book Processor from Elcomsoft. These devices have "fair uses", even if the consumer can make a digital copy with no quality degradation. One such example is to open an e-book on a Macintosh or Linux computer.

Lets face it, just because a device can allow the consumer to make a perfect copy does not mean it should be banned. If that were true, the photocopier should be banned too! If one puts money, or a government document into a color copier, this does not stop it from copying it, doesn't it? Plus, there is nothing in the copyright law that says that a consumer made copy has to be lower in quality than the original. It is a common industry myth that this is true, but it is not. A "fair use copy" can be in perfect, digital, form. The consumers are infuriated, and they do not want to buy the products of the people putting out this propaganda.

How the labels pay subscription services are no comparison to the content and catalog offered on most Peer-to-Peer systems today:

First of all, the *catalog of content* offered on the labels sites (such as MusicNet, PressPlay, FullAudio, and Rhapsody) is no comparison to the catalogs of P2P systems like KaZaa, Gnutella, Blubster, and Morpheus. In addition, many "licensed" services have tracks just from a few labels, and just selected tracks from those labels. Many people, who use the "licensed" services, have to subscribe to many different services to get the music they want.

Next, many "licensed" services use *encrypted file formats*, which make the files *unusable* with many media player programs, CD burning programs, portable player device and many non-windows operating systems (such as Mac OS, Linux, BeOS, Lindows, Unix, etc). Often, the formats of the licensed services are specific to a service, and the user cannot organize all their tracks easily. For example, MusicNet uses RealAudio format, which means you must use the Realone player to play your tracks, and it offers tracks from BMG, EMI, Warner Bros, and Zomba. Next, you also realized you want some Willie Nelson, which is on Universal. You then subscribe to PressPlay, and find out that your Realplayer cannot play the tracks, and you must now use Windows Media Player. Now, you learn that you have to subscribe to TWO services, and have to use TWO different media players, so you cannot play one after another in a play list, since the files are incompatible.

However, if the same user were to download LimeWire, Morpheus, or KaZaa, they would have found the same musical groups in a format (most likely MP3 or OGG), which many media players can play. It is more of a "one stop" place to find the content they want.

Many label owned services usually limit the bit rate that files can be downloaded it. Most label owned services offer between 64K and 160K bits per second. Most P2P systems offer higher bit rates, which means the sound from the files is generally

better. It is not uncommon to find files ranging from 128K to 320K on LimeWire and Grokster.

Next of all, most people who download expect to be able to use the files they download on their portable players. Like I have said above, most people want to download the music they have and use it on their portable player. Many people prefer to download than "rip", because it is easier. Most label-owned services offer little or no ripping capability. Even porting of MPEG video to portable devices is becoming more common. Most Laptop computers will play MPEG videos. Archos is making a handheld device that can play MPEG, and other video files. People often take portable devices in cars, airplanes, to the office, jogging and other places, because they can hold a lot of music and other content, and are easy to use.

I, and other people I have talked to, are dissatisfied with the security (copy protection) of most label owned music sites, because it impairs the users ability to make a backup copy of their downloads. Consumers should have the right to backup their paid-for downloaded content to floppy disks, Data CDs, Zip Disks, Tape Drive, RAID Drives, Network Backup Systems, and other media, and be able to restore it without wasting a license, or the content becoming unusable after the restore.

This "anti-copy" technology also has other drawbacks. You are not allowed to "move" the content you legally have the rights to play to another computer (such as your laptop, or when you upgrade, and the like. It also prevents many Macintosh and Linux computers from even being able to play it. For users at work, and the like where their "My Music" folders are stored on the network server (such as with Windows/Novell/Linux domain controllers), it disables them almost instantly, because of the syncing involved.

Consumers want to be able to keep the content they download. Most pay services have the content "self destruct" after a set number of days, becoming a non-subscriber, or after a set number of plays. Most P2P systems offer "unlimited play" content. Many people I know are proud of their digital libraries, and do not want to have to pay more fees to play their content down the road, especially users with slow modems.

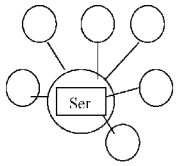
Last of all, many people expect to be able to CD/DVD burn the music or movies they download. People have expected this since Napster, and they will continue to do so. Most people are likely to pay for "newfangled" stuff, not "limited use" stuff.

Service	Type	Catalog Offered	Company	File Format	Tracks Copy Protectd	Portabl Player Use	CD Burn-Able	Artists Paid	Track Play Time	Price
Kazaa	Hybrid P2P	Most Major / Indie Labels	Sharman Networks	MP3, OGG, WMA, MIDI	NO	Yes	Yes	No	No Limit	Free
LimeWire	Decentralized P2P	Most Major / Indie Labels	Lime Wire	MP3, OGG, WMA, MIDI	NO	Yes	Yes	No	No Limit	Free
SongSpy	Centralized P2P	Most Major / Indie Labels	IDG Entertaiment	MP3	No	Yes	Yes	In the Future	No Limit	Free
Morpheus	Decentralized P2P	Most Major / Indie Labels, Unsigned Bands	Streamcast	MP3, WMA, OGG, MIDI, Morpheus	Selected Tracks	Selected Tracks	Most	Some	Some have Limits, some not	Free
Blubster	Decentralized P2P	Most Major / Indie Labels	Blubster	MP3	NO	Yes	Yes	No	No Limit	Free
GiFT	Decentralized P2P	Most Major / Indie Labels	<Open Source>	MP3, OGG, WMA, MIDI	No	Yes	Yes	No	No Limit	Free
Emusic	Server Download	Select Indie Labels, Universal	Vivendi Universal	MP3	NO	Yes	Yes	Yes	No Limit	$9.95 - $14.95
MusicNet	Server Download	BMG, EMI, Warner Bros, Zomba	MusicNet	Real audio	Yes	No	No	Yes	30 Days	$9.95
Pressplay	Server Download	Sony, Universal, Zomba, EMI, TVT	Pressplay	WMA	Yes	Selected	Selected	Yes	Until cancel	varies

How P2P is not a "Company Controllable Medium":

Peer-to-Peer means in reality "consumer to consumer, with no middleman. In many of today's P2P networks, there is not any company responsible for the content. In a P2P system, you are dealing with 3 separate "entities", the software creator (who creates the actual P2P software program), the directory system (which inventories the files of the various computers sharing data), and then the nodes (which are the actual computers sharing data with each other), many of which can be individuals, companies, or automated functions.

In *Centralized* P2P systems, the directory system is usually run by a company or individual, where all the nodes connect to a central server, and the central server "catalogs" what files the users are sharing. This medium is easily controllable for copyright infringement, because blocking can be installed. Napsters, Opennap, Scour, are examples of this system. Below, shows the model of a centralized P2P system:



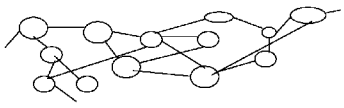
With the response to the Napster and Scour lawsuits, most P2P systems are *decentralized* these days. This means that all the nodes do not go through a central server. Instead, the directory system, either involves *sequential broadcasting* (as in Gnutella, LimeWire, Blubster, etc), or *"Supernode Hubs"* (as in KaZaa and Grokster). This means that the directory, uploads, and downloads are all done without the use of a central login server. This results in a total disconnection from the system developers and the users. Often every node is a client, server, and a directory station. The computers *connect directly with each other*, without a central point.

When most people launch a decentralized P2P client, it tries to connect a list of hosts (i.e. other computers running the same piece of software at the same time), till it finds one. This "list of hosts" is stored locally on the user's computer. Sometimes servers or other hosts store lists of hosts, and searches come through to them. Once a few hosts are found, and the user is connected he/she can search for content. If a host is not found, the user in many cases can manually enter the IP address and port of another user.

When a search query, is executed, the computer sends it to his/her connected hosts. If anything is found in their shared folder, it is sent back. It then broadcasts the query to any other hosts those hosts are connected to. This continues many levels deep. Since many computers are connected to different hosts, the search continues.

When one chooses a file from a search that he/she wants, the hosting computer is told to upload a copy of it to the computer that requested it. One the next page, there is a diagram of a decentralized system.

A Network diagram of a decentralized P2P system:



This decentralized design means that "spying", monitoring users conduct, censoring copyrighted content, and the like nearly impossible. Since there is no company or government "middleman", these networks are almost unstoppable. A lawsuit would be useless in stopping this kind of network. As you can see from the diagram, there is no one node that can turn all the other nodes off. These networks are very fault tolerant.

With some networks (such as Nucleus and giFT), having open source code, it means that the *creators are individuals*, not companies. This means that they probably do not have $150,000 for each work infringed on their networks, for files they did not share themselves. Even if the creators of a network go bankrupt, the software loaded on client hard drives will still work. This means that these networks have the potential to work almost forever, and they should be used to their biggest advantage.

Compensating Creators in a Peer-to-Peer world:

Since copyright is not always enforceable in a peer-to-peer world, there are various approaches to compensate artists and other content creators for their work downloaded on P2P networks. The music and movie industries are concerned that artists, and producers will never be paid, and P2P results in "theft" of their content. They also claim that it bypasses their "monopoly distribution control".

Many content creators need to make a living. An artist's job is to perform music. A songwriter's job is to create songs. TV-Show producers and movie producers deserve to be paid for their work. There are many ways to compensate the creators in a P2P world. Many of the schemes would even work on an open source, decentralized system.

For centralized systems, the easiest way is to license content to the P2P company, and charge for access, or sells banner or pop-up ads. SongSpy, and Scour are doing this now. Right now, it is hard for independent companies (i.e. not owned by RIAA or MPAA member companies) to get licenses for major label music. In addition, the Musicnet/PressPlay exclusive contracts generally make it hard for one to get licenses from all the labels. The Music Online Competition Act, proposed by rep. Rick Boucher, and rep. Jack Cannon would ease this licensing hassle. Ultimately, compulsory licensing may be the only solution to really fix the problem.

The Department of Justice is currently investigating the labels licensing practices. The RIAA represents foreign corporations, such as Sony, which is based in Japan. In addition, the record labels are being investigated for fraud. They are trying to monopolize all 'new media technologies", to the point in which new mediums *cannot be invented by non-member companies*, or without their permission.

For the decentralized systems, compensation is a little bit harder. However, myself, along with Ian Clarke of Freenet, and Matt Goyer of Fairtunes, beleive that it is possible to "reward artists without copyright". There are many ways of doing so, even if a company does not run the distribution system.

Fairtunes (now MusicLink) created an "artist tipping" system. This system allows one to use their credit card, and Fairtunes would send a check to the artist or songwriter. Some clients like Kick and Freeamp, have built in Fairtunes/MusicLink tipping. This has generated many thousand dollars to artists by people giving voluntary compensation. Adding this kind of a feature to any P2P system (including decentralized systems) is easily doable. Many artists believe that the current system of copyright and label ownership is failing to reward artists. On VH-1s show "Behind the Music", you hear story after story of artists being "ripped off" by the music industry.

Another way of compensation that I propose myself, would be to embed royalties in the price of BLANK CDs, DVDs, MP3 Players, and the like. This could generate a lot of revenue, and for each "royalty paid" disk, you get a license to fill it up with content from P2P systems, "rips", and other content.

Another way that I thought of would be to tax Internet service. If each user paid a monthly fee of $0.35 for dial up connections, and $1.00 per month for broadband, this would generate tens of millions of dollars per month, or billions annually. These royalties could be passed on to artists, songwriters, TV show producers, movie producers, movie studios and the like. I think that a reasonable distribution of these "taxed" funds, should be a 47-47-6 distribution. That is 47% of the money go to the individuals that create the content (i.e. artists, songwriters, actors, producers, etc), and 47% to the companies that create the work (such as labels, publishers, studios, game companies, etc), and leave 6% for independent, unsigned groups (such as independent filmmakers, unsigned bands, garage bands, local bands, K-12 Music Programs, College Music Programs, church choirs, youth choirs, etc).

The system should have a means to get these royalties to the parties, quickly and efficiently. If the payments are through an agency, it needs to be totally neutral (i.e. not owned by any artist, songwriter, record label, music publisher, movie studio, game company, or lobby or trade organization). An independent organization along the lines of ASCAP or BMI would be best in my opinion. In any case, it should be frequently and publicly audited.

Fair Use and how Digital Rights Management is not the solution to this P2P issue:

First of all, digital rights management (DRM) is designed to restrict use, not to benefit the consumer. This technology limits use, and in fact often alienates the consumer. The next problem is that DRM in not secure forever. All DRM is hackable in some form. Last of all, according to Professor Leland Beck at San Diego State University told me that "encryption" is not a good copy protection system, because it *does not prevent bits of data from being copied at all*, it only prevents *reading and decoding of data*.

The nature of digital technology is that every bit of information is encoded into ones and zeros. This means that all that any digital chip can detect are ones and zeros. This makes "perfect" copies the norm. If you can find every bit that a medium can detect, and put it to the exact same location on the destination, the copy will be seen as an original.

People have used copy protection technology for years. Back in the Apple II days, copy protection on disks was the norm. Yet, people and companies figured out the protection systems, and wrote software that would copy it. *Central Point Software* wrote a new version of *Copy II*, every time a new protection system was released that would copy those protected disks. Also, people rejected the copy-protected disks, and some customers refused to buy copy-protected software if there were an unprotected competitor. A court case in 1984 proved that a program that copied protected disks could be sold, since it allowed the user to make backup copies.

The music industry should have learned that copy protection is hacked quickly. It took Professor Felten and his students only a few weeks to crack the Secure Digital Music Initiative (SDMI) audio watermark schemes. Beale Screamer created a utility called FreeMe that unprotects WMA audio files. It did not take screamer long to crack that.

Even encryption built into hardware can be cracked. Many coin-op arcade games had hardware DRM built into them. Yet, many of them have been cracked, often within a few months after the release. Many emulator developers have also cracked arcade games to play them on a PC. Team CPS2Shock figured out a way to decrypt games on the Capcom Play System 2 Arcade System by using some code of their own in RAM on the board, and some wiring to a PC. The DVD encryption was figured out by a 16-year old named Jon Johansen to play his DVDs on a Linux computer.

Next of all, the DRM is only as good as a player that honors it. For example, if one has a sound card with no digital "record back" disable, and one "records" the protected content back to disk and saves it as MP3, they can now share it over Gnutella. Even connecting the analog out to another computer's analog in is a way to unprotect content.

Lets face it no DRM system is secure forever. Mandating security standards into computers, like the Hollings Bill would require would just cause the consumer frustration, and that it will encourage a hacker to figure it out. Also, new formats will not be secure with old DRM chips. Michael Eisner from Disney was asked, what if one records a movie in a theatre, saves it in a format the DRM in the computer does not recognize, and then shares that file over Gnutella? His answer is "nothing"!

Last of all, DRM limits fair use. People have "fair use rights", to time shift, space shift, to reverse engineer, to quote, and the like. Limiting these creates headaches for a lot of people. Being locked out of content will just ENCOURAGE hackers to break the DRM code, just like prohibition did with liquor in the 1920s.

DRM will not solve the P2P issue. It will just encourage the development of unprotected formats. Even if illegal, people will download and create these formats anyway. In my opinion, there is no way to stop a consumer getting an unprotected, perfect copy of content in the digital world.

Spying on consumers as "copyright police" is not a viable option too. This option is expensive. It also violates ones rights to "innocent until proven guilty", "right to a fair trial", and the like

Placing "Spoof" files on P2P networks that contain 30-second loops or 3 minutes of silence is not a long-term solution either. It just infuriates the consumer, and does not stop them from downloading "real" content files. Also, it is encouraging the development of blocking systems that the consumers are using to block known "spoof IP Addresses".

Conclusion:

I hope that congress takes my input, and puts P2P to good use, and understands how it benefits all, including consumers, artists, and the like. I do not think it is worth banning, and it should be legal to use it, and not have the content available on P2P Networks censored or controlled by large corporations.

PHILIP S. CORWIN

BUTERA & ANDREWS
ATTORNEYS AT LAW
1301 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, D.C. 20004-1701

TELEPHONE
(202) 347-6875
FACSIMILE
(202) 347-6876

PCORWIN@BUTERA-ANDREWS.COM

Date: October 9, 2002
To: Members, House Subcommittee on Courts, the Internet and Intellectual Property
From: Philip S. Corwin
Subject: Correction of the Hearing Record

I am writing on behalf of our client Sharman Networks, the owner of the KaZaA.com website from which the KaZaA Media Desktop peer-to-peer software is made available for downloading. On September 26, 2002, during the Subcommittee's hearing on "Piracy on Peer to Peer Networks", Ms. Hilary Rosen of the Recording Industry Association of America delivered testimony that contained the following statement: *An example of why it is so important to give copyright owners the ability to defend themselves with the same technological measures used by pirates to encourage theft came just this week when KaZaA announced that it was giving its users "better options and more tools than ever before ... include[ing] a filter to help users avoid ... misnamed or incomplete files that may have been uploaded by record labels and copyright owners trying to frustrate file sharing."*

Ms. Rosen's statement makes it appear that KaZaA had publicly stated everything enclosed within the quotation marks. However, neither Sharman Networks nor KaZaA ever made any such statement.

The September 23rd press release announcing the launch of KaZaA V2 is attached. As you will note, Sharman CEO Nikki Hemming did make the statement "We've given users better options and more tools than ever before", but did not say any of the other words attributed to her by RIAA in this alleged quote, which was reproduced in a poster that was conspicuously displayed at the front of the Judiciary hearing room. We have been unable to locate any news story or other source for the quote attributed to KaZaA by the RIAA, and can only guess that they spliced together this portion of the press release with an incorrect characterization of the software's purpose written by a third party.

Sharman does not condone or encourage copyright infringement. In fact, the KaZaA home page as well as the User License Agreement expressly admonishes persons who have downloaded the software that they are responsible for complying with their home country's copyright law.

We do not know whether the RIAA's misattribution of this statement was inadvertent or was deliberately aimed at inciting the Subcommittee against our client. We did wish to set matters straight, and ask that this communication be made part of the official hearing record. Thank you.

Contacts:
Kelly Larabee
The Rose Group
+1-602-258-1416/+1-310-280-3710
kelly@therosegrp.com

FOR RELEASE 8:00AM EST

SHARMAN NETWORKS LAUNCHES NEW VERSION, KAZAA V2

Industry-Leading File-Sharing Program Adds Unique Functionality

LOS ANGELES – (September 23, 2002) – Sharman Networks Limited today releases Kazaa v2, the latest version of its Kazaa Media Desktop (KMD) software. With more than 120 million downloads to date, KMD is the peer-to-peer application of choice for multiple forms of digital media. Kazaa v2 sets a new standard for peer-to-peer functionality.

"We've given users better options and more tools than ever before," said Sharman Networks CEO Nikki Hemming. "Shared playlists lets them promote collections of their own work, participation levels rewards those who contribute and anti-virus measures improves security."

Building upon the success of previous versions, Kazaa v2 introduces a host of new features.

- Web Search: Use standard KMD interface to search the Web.
- Customizable Skins: Change the basic desktop interface with a skin, giving different layout and display options. One skin comes with KMD and two more can be downloaded. More skins will be released soon.
- Shared Playlists: Create unique shared playlists of your own content and share it as a collection. You can also search for and download compilations of files created by other users and premium content providers.
- Improved Image Handling: More image formats supported through the Theater view.
- Integrity Rating: Files rated by peers according to technical quality and completeness of meta data. This will improve reliability of files, and reduce the likelihood that low integrity files will be shared.
- Participation Level: Users frequently sharing their own content and rating files are rewarded with higher priority in download queues to encourage positive contributions.

- Integrated Anti-Virus Protection: Shared folders can be automatically scanned on startup of KMD and during each download for greater protection against infection and spread of viruses.
- Expanded Online Help Section: Kazaa.com offers quicker orientation for new users with a new user page, Quick Guide, User Guide, and updated FAQ.

Business Relationships
Sharman's stated commitment to expand Kazaa Media Desktop user benefits has resulted in best-of-breed offerings from key allies in a variety of categories. Newly formed strategic relationships include:

- **Music** - Cornerband.com, an online music community, which offers KMD users the opportunity to experience emerging bands and vote in the 30 Best-Bands promotion, while giving subscribing musicians an opportunity to promote, sample and sell their music
- **Anti-Virus** - Bullguard, a leading Internet security provider, which delivers anti-virus protection and offers full-suite security solutions to users
- **Broadband** - Tiscali, one of the largest Internet service providers in Europe, offering broadband Internet for peer-to-peer users

Additionally, Kazaa Showcase launches with links in KMD to premium content such as the latest music, video and software from Altnet.

About Sharman Networks Limited
Sharman Networks Limited distributes the popular Kazaa Media Desktop software, the leading peer-to-peer file transfer application that allows users to search, download, organize and interact with a variety of files. Founded in 2002, Sharman Networks is a consortium of private investors with multimedia interests. Sharman Networks provides distributed computing software applications that are pioneering the digital revolution. Sharman Networks is a worldwide operation, based in Australia, with offices in Europe. For more information about the Kazaa Media Desktop, Sharman Network's leading P2P software application, please visit Kazaa.com.

###

September 20, 2002

United States House of Representatives
Committee on the Judiciary,
Subcommittee on Courts, the Internet, and Intellectual Property
2138 Rayburn HOB
Washington, DC 20515

Re: September 26, 2002 Hearing on Peer-to-Peer Networking

Dear Members of the Subcommittee:

I am writing to express concern about a bill now pending before the subcommittee, the Peer-to-peer Piracy Protection Act (H.R. 5211), and to bring to your attention an aspect of this proposed legislation about which you may not yet be aware. Specifically, I want to call to your attention the real and critical importance of peer-to-peer networking technology to our nation's economy and to domestic and international security.

My views reflect nearly 25 years' experience in the computer industry. Among other significant experience, I created Lotus Notes (an IBM product), a communications software application now in use by more than 85 million people worldwide. I oversaw the development of Notes for thirteen years, from its inception in 1984 through 1997. Major corporations, small businesses, civil, military and intelligence agencies, and individuals use Notes for its e-mail capabilities and to share information, data, files, and other resources.

In 1997, I founded Groove Networks, Inc. to develop a new class of computer networking technology designed in part to overcome many of the security limitations inherent in the client-server architecture on which Notes is based. I came to realize that much of the most important work being done by our customers – whether businesses or governmental agencies – occurred within formal or *ad hoc* teams of individuals who communicate, largely over unsecure e-mail, within and beyond organizational boundaries. As explained below, our product Groove (which is five years old, and two years in the marketplace) is based fundamentally on a peer-to-peer architecture specifically because this architecture facilitates the types of secure, dynamic, inter-organizational communication and collaboration that client-server technologies such as Notes cannot support.

Although our work on Groove predated Napster by years, peer-to-peer technology unfortunately has become synonymous with Napster and other music file-sharing applications. Napster captured the public's attention because it satisfied an immediate desire of its users – to find and download music - and not because it is peer-to-peer technology. Peer-to-peer technology is about much more than music file sharing, and Napster was held liable for its intent and conduct in creating and operating a service designed specifically for unrestricted public swapping of music, *not* because of the peer-to-peer architecture of its software.

Peer-to-peer is a generic term for any use of a network that enables computing devices ("peers") to interact directly, without assistance (or with minimal assistance) from central computers (*i.e.*, servers). Peer-to-peer technology with file sharing functionality predates Napster by nearly three decades. E-mail, which was developed in 1971, adding messaging and file exchange capabilities to the federal government's ARPANet network, is fundamentally a peer-to-peer technology, using servers only as intermediate "post offices." Peer-to-peer local area network operating systems were introduced in the early 1990's (Artisoft LANtastic, 1991; Microsoft Windows for Workgroups, 1992). Lotus Notes used (and continues to use) a peer-to-peer file and data replication scheme to synchronize between servers. The development of Groove, which began in October of 1997, was based upon a solid foundation of prior peer-to-peer technology research and practice – all of which significantly predate Napster's 1999 notable debut that brought the technology to the forefront of popular culture.

Groove Networks
100 Cummings Center
Suite 535Q
Beverly, MA 01915

T 978-720-2000
F 978-720-2001

Peer-to-peer networking technology enables many forms of content-neutral peer interaction that represent important new uses of the Internet, many of which enable file sharing. The following are among the many new uses of peer-to-peer technology:

- Secure communication and collaboration among groups, a.k.a. "groupware" (*e.g.*, Groove, Ikimbo, and Magi Enterprise)
- Online product and services marketplaces and supply chains (*e.g.*, FirstPeer)
- Online education and distance learning (*e.g.*, Colloquia)
- Secure health care information exchange (*e.g.*, CareScience)
- Intra- and inter-organizational content and knowledge management (*e.g.*, NextPage)
- Pooling of distributed computer processing capabilities, a.k.a. "grid computing" (*e.g.*, seti@home for astronomical research and United Devices for use in the search for cures for disease and other scientific endeavors)
- Messaging (*e.g.*, Jabber)
- Computer games (*e.g.*, Quazal)
- Secure distribution of licensed media and intellectual property (*e.g.*, Akamai and RightsMarket, Inc.)

A peer-to-peer architecture is used for these purposes and many others because peer-to-peer networking has numerous advantages over server-centric technologies for critical information sharing activities. For example, peer-to-peer networks can have no single point of failure – a fact that is of critical importance to the military, intelligence agencies, disaster response agencies, air traffic controllers, and others who need fail-safe forms of communication, collaboration, and data and file trading. Peer-to-peer technology also can enable greater network security and superior protection of intellectual property. When data is encrypted end-to-end and transmitted on peer networks, data can be more difficult to intercept because the encrypted data in transit can be made invulnerable to disclosure, and interruption of transmission can be far more difficult to accomplish because data need not follow a predictable path to-or-through a central point. And, with a peer-to-peer communication and collaboration program like Groove, small businesses, individuals within larger organizations, and autonomous individuals (from independent consultants to FBI agents in the field) can instantly create *ad hoc* networks for rich forms of information sharing, all without having to buy and set-up computer servers, which often requires costly and time consuming technical support.

Businesses and government agencies have invested in peer-to-peer technology such as Groove because it protects their information and intellectual property better than systems built upon alternative technologies. By using it, they eliminate potential points of vulnerability to attack in attempts to obtain or deny access to their intellectual property. Perhaps more aptly stated, the decentralized aspects that make peer-to-peer technology challenging from an intellectual property control standpoint to some, are *precisely* the things that make it desirable and valuable from an intellectual property protection standpoint to others.

A recent Gartner Research Note (Technology, T-16-2550, Sept. 16, 2002) predicts that, "[b]y 2005, 10 percent of business interactions will occur via P2P-enabled technologies (0.7 probability)." The following are a few examples of some current uses of Groove explored by hundreds of thousands of individuals and hundreds of organizations and agencies worldwide:

- DARPA is using Groove extensively, as are a number of major defense contractors, in developing applications for cross-agency (defense, intelligence, NGO) collaboration in analyzing and acting upon security threats
- Major commands of the United States Department of Defense and several branches of the military are actively exploring a number of uses ranging from command to telemedicine
- Major pharmaceutical companies (*e.g.*, GlaxoSmithKline) are using Groove for inter-organizational collaboration related to the development and approval of new drugs
- Two large, global enterprises are using Groove to plan the post-merger integration of their combined operations
- College professors are encouraging students to use Groove for online study groups
- United Methodist pastors have explored using Groove to coordinate work in a rural area of South Georgia

All communications and computing technologies can and will ultimately be used for ill and good, and some content-neutral devices and peer-to-peer networks occasionally *will* be used for illegal purposes. And the more security that these networks offer to their customers, by intentional design, the closer to impossible it

becomes to distinguish the good activity from the ill. The forms of self-help that H.R. 5211 authorizes would likely disable general-purpose peer-to-peer networks, preventing or severely hindering extant and future legitimate uses of them. H.R. 5211 is not specific about the forms of self-help that copyright holders would be permitted to exercise, but it generally would authorize copyright holders to use technologies designed for purposes of "disabling, interfering with, blocking, diverting or otherwise impairing the unauthorized distribution, display, performance, or reproduction of his or her copyrighted work." While H.R. 5211 theoretically does not permit copyright holders to impair other files or data or interfere with the activities of those who share a peer-to-peer network with illegal file-traders, it is difficult to imagine how these problems could be avoided in practice. To function within the parameters that H.R. 5211 attempts to establish, self-help technologies must have at least some visibility into the substantive content of data or files, in order to determine infringement. But the data security functionality of some peer-to-peer information sharing and collaborative work technologies, such as Groove, would make it extremely difficult if not impossible for self-help technologies to distinguish infringers from noninfringers. Furthermore, even if accurately targeted, self-help technologies specifically intended to stop unauthorized distribution of copyrighted works through "denial of service" methods would almost certainly impede the service of other innocent users unknowingly sharing communication networks and infrastructure.

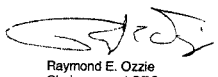
Perhaps most disturbing is the "chilling effect" that legislation might have on technology that is critical to information security in business and government. Even a reasonable fear of recurring attack on shared public infrastructure is likely to discourage legitimate uses of peer-to-peer technology.

We believe strongly in targeting and penalizing illegal behavior, as opposed to targeting multiple-use technology that reasonably and uniquely serves secure information-sharing needs. Not that technology is irrelevant, of course: it can also play a role in discouraging illegal behavior, *e.g.*, through use of Digital Rights Management technology, which the Groove software and many other products support. But there are also approaches under existing law, including use of lawsuits against those who infringe others' copyrights, whether directly, vicariously, or contributorily; and resorting to the remedies established by the Digital Millennium Copyright Act.

Thank you for taking the time to consider my views on H.R. 5211 and the important topic of peer-to-peer technology. This technology is beginning to make important contributions to our economy and to national security, and I am certain that it ultimately will become a critical component of the world's communication and computing infrastructure.

I would be grateful for any opportunity to be helpful to you as you continue to consider the important subject of peer-to-peer technology, whether by providing additional information, meeting with members of the subcommittee, or testifying at any subsequent hearings. I would appreciate it if you would include this letter as part of the official record of the subcommittee's September 26, 2002 hearing on the issue of copyright infringement on the Internet.

Sincerely,



Raymond E. Ozzie
Chairman and CEO

PREPARED STATEMENT OF PANOS ANASTASSIADIS

Thank you for the opportunity today to submit our insights regarding piracy on distributed Peer-to-Peer networks.

Cyveillance is engaged in providing Internet Intelligence services to a client list that includes 19 of the Fortune 50 companies, and I assure you that all of these firms share the same concerns regarding the theft of intellectual property via the Internet. In fact, what drives our business success is the huge potential that exists today in recapturing revenues lost due to such activity.

Our services are underpinned by patented technology that scours the entire Internet and delivers distilled, 100% relevant intelligence provided in a prioritized manner that can be readily acted upon.

It is interesting to note that distributed Peer-to-Peer networks are only one portion of the Internet that experiences traffic in IP theft, even though they by far experience the highest volume of such activity. Web sites, message boards, IRC chat, FTP, newsgroups and auction sites all experience their share of discussion and participation in the theft of Intellectual and Physical property.

The size of the piracy problem itself is not a new discussion topic. And the medium that has received the most press to date—helped along by the Napster case—has been music. But, as we know with anything facilitated by technology or the Internet, the issue has spread and evolved rapidly.

Today for example, it is estimated that over 20 million movies are being downloaded each month. Billions of dollars of intellectual property from the largest businesses in the world are impacted by IP theft to include music, motion pictures, games, software and ePublishing. The most trafficked area of the Internet for such illegal activity is on distributed Peer-to-Peer networks; just yesterday, September 25, the most active distributed Peer-to-Peer network had 2,940,981 users online, and that was just one network.

We use the term "distributed" Peer-to-Peer network because there is a difference. For example, Napster (not "distributed") faced a legal challenge that centered around the means of distribution and how the files were managed. In the Napster case, file catalogues were **centrally** housed and managed. On true "distributed" Peer-to-Peer networks however, there is no centralized catalogue and the network owners clearly state that they have no control over content.

Distributed Peer-to-Peer networks and the efficiencies of their architecture provides many positive benefits to the online community as a whole, although sharing legally-protected intellectual property is not one of them.

For the rightful owners of intellectual property, effectively addressing the piracy issue is not a singular effort but a multi-pronged approach. As a leader in Internet Intelligence, our experience has shown that a best-practice approach will include a number of components:

1. Further **educate** consumers on the fact that downloading proprietary content is not "ok." *An entire generation of users has grown up under peer assumptions that there is nothing wrong with downloading proprietary content.*
2. Gain **awareness** of the size and scope of the problem through technology monitoring. *You cannot manage what you cannot see. This can only be accomplished through proven Internet Intelligence technology.*
3. **Enforce** and protect what is rightfully identified as IP theft. *Not taking action is not an option.*
4. Offer reasonable and **legal alternatives** to obtaining quality files and IP. *The industries experiencing theft must come up with reasonable legal alternatives before the public will adopt proper channels of obtaining content. " Reasonable" includes pricing that compensates the owners and distributors, but reflects the lower cost of distribution over the Internet, thereby creating a win/win with consumers.*
5. **Measure** the size of the problem on an ongoing basis. *Employ technology to monitor success and trends.*

In order to realize the benefits of such a plan as described, businesses should not be handicapped in their ability to work with effective self-help technology measures that cause no damage to non-offenders on the networks or the networks themselves. These barriers should be removed by the modification of the Digital Millenium Copyright Act (DCMA) to include notice on distributed Peer-to-Peer networks.

for Competitive Technology

September 25, 2002

Howard Coble
Chairman

Howard L. Berman
Ranking Member

Committee on the Judiciary
Subcommittee on Courts, Internet, and Intellectual Property

VIA ELECTRONIC MAIL

The Association for Competitive Technology (ACT) submits the following paper on H.R. 5211 and the subject of protecting digital content on peer to peer (P2P) networks. ACT represents over 3,000 information technology (IT) companies and professionals involved in creating solutions for the transmission of digital content. Like you, we strongly believe that the marketplace, without the assistance government technology mandates, is in the best position to respond to the demands of consumers and copyright holders.

ACT has previously stated its general support for H.R. 5211 legislation designed to curtail the spread of illegally acquired copyrighted works. Piracy is a significant challenge for the digital media and IT industry and we applaud your effort to promote technological rather than regulatory solutions. I must qualify this support by pointing out that when crafting copyright legislation, we should maintain a dialogue to avoid untended consequences that could harm small IT companies.

There is an estimated $270 billion market opportunity for digital content. The key to this opportunity will be effective, consumer friendly Digital Rights Management (DRM) technologies and solutions. The technology industry is already hard at work to take advantage of an estimated $3.5 billion market for DRM software by 2005. Without a doubt, the emerging and maturing DRM technologies created will enable secure electronic content, in part by providing copyright holders a method to identify and impair the transfer of pirated content via peer to peer networks.

Clearly, if legislation to prevent copyright infringement is to work its way through the legislative process, it will have to do so in parts. For example, congress has made the conscious decision to trifurcate the process by addressing the broadcast flag, analog hole and P2P issues separately. This approach demonstrates the vast complexity of crafting a solution while at the same time pointing out the folly of the one size fits all government technology mandates method. We believe your approach focuses on encouraging technological solutions and is far superior to the attempts by some in Congress to who would rather institute government technology mandates.

P2P file sharing systems are on the cusp of becoming an important platform for innovation. P2P networks are designed to utilize the storage capacity and power of individual PCs to accomplish tasks once limited to servers and mainframe computers. It is our belief that the deployment of specialized technologies that have the ability to affect the spread of unauthorized content will not have the deleterious effect on P2P networks as claimed by those in opposition.

ACT appreciates the Subcommittee's effort to building a strong record of this bill's intent to encourage the use of market based technology, rather than government mandates, to protect the interests of copyright holders.

Sincerely,

Jonathan Zuck
President

1413 K Street, NW * 12th Floor * Washington, DC * Tel: 202-331-2130 * Fax: 202-331-2139 * email: info@ACTonline.org * www.ACTonline.org

Association for Competitive Technology Briefing Paper:
Solving the P2P piracy issue through technology "self help"

Over the past year, the collision of copyright law and emerging digital technologies has become one of the most divisive issues in Washington. In today's environment, it is nearly impossible to get beyond the rhetoric and have an intelligent discussion about this extremely important issue. The Berman P2P bill (H.R. 5211) is no exception and this paper is an attempt to "step back from the ledge" and inject a dose of clarity into the debate.

1. Separating the Rhetoric from Reality

Despite the red hot rhetoric and creative use of examples from both sides, H.R. 5211 is actually a reasonable piece of legislation. While the legislation is not perfect, it is a noble attempt to fix a very real problem. In this case, it is the rhetoric from the other side of the debate, some from our very own industry that needs to be dispelled.

Many opponents of the bill including the trade association representing Morpheus, the Computer and Communications Industry Association (CCIA), have labeled this a "cyber vigilante" bill. Contrary to these brazen claims, H.R. 5211 attempts to strictly limit the use of technological tools *by copyright holders* to enforce their legal rights. This accusation completely misses the mark. H.R. 5211 is only allowing copyright holders to avail themselves of tools to protect the rights *they already have*. Indeed, these actions are easily distinguishable from the history of vigilantism.[1]

For a bit of historical context, consider the San Francisco vigilantes that sprung up around the time of California statehood. Local citizens had become so impatient with the inability or unwillingness of local officers to enforce the law that they formed a "Vigilance Committee" to administer justice. By the time that the committee disbanded at the end of September, they had hanged four men, handed fifteen over to the police for trials, and whipped or deported twenty-nine more. These actions can be classified as "extrajudicial" at best and in no way analogous to the self help concept behind H.R. 5211. For example, H.R. 5211 subjects the lawful copyright holder to an *additional* cause of action if it acts outside the protections of the 514(a) safe harbor. Moreover, the copyright holder must clear the enforcement tool with the Department of Justice *before* it is deployed. In other words, there is no opportunity for the rights holder to administer "frontier justice" with out incurring considerable legal exposure. Ironically it could be argued that pirates may be the ones that band together to seek out copyright holders who are acting within their rights and bring them up on charges.

Another objection that has been raised is that the law will get applied outside of P2P networks and include email and other platforms of potential use in file sharing. First, the bill deals directly with P2P networks and file sharing but once again, any tools need prior approval by the Department of Justice, rendering some of these specious claims moot. Furthermore, there are practical implications to these predictions. Monitoring of email for copyrighted content is problematic at best, given legal restrictions and encryption and other tools, especially when you consider the rather inefficient means of file sharing that email represents. Instead, it is far more likely that content owners will target blatant "low

[1] See, e.g. "California as I Saw It:" First-Person Narratives of California's Early Years, 1849-1900. National Digital Library Program, Library of Congress.

1413 K Street, NW * 12th Floor * Washington, DC * Tel: 202-331-2130 * Fax: 202-331-2139 * email: info@ACTonline.org * www.ACTonline.org

hanging fruit" such as Morpheus whose entire raison d'etre is the illegal distribution of copyrighted material.

Another red herring introduced by those who favor undermining copyright protection, is that this legislation will spur intervention on the part of everyone seeking to protect their copyrighted material. Since every work is, by default, copyrighted, the scenario is that we will become a society of people scouring the web for illegal copies of our works. Once again this hyperbole is a clear attempt at misdirection. First of all, everyone has a legitimate interest in protecting their copyrighted material but as a practical matter most of us don't bother if there are no economic implications. The likelihood of everyday citizens contacting the DOJ to gain approval of an interdiction tool to control the distribution of their public postings seems pretty low.

The basic premise is that copyright holders will now begin to enforce their copyrights, rights that have been upheld in the courts. The notion that this is somehow bad is hard to stomach.

Copyright law and policy involves a relationship between rights holders and consumers. Indeed, consumers, through statute and case law, have come to expect certain fair use rights. However, the entities that are engaged in the activism addressed by this bill are not "consumers" in the sense of copyright policy, nor are their activities the type envisioned by the fair use doctrine. These entities are engaged in the piracy of intellectual property, pure and simple.

Copyright confers exclusive rights to the author of the particular work. Two of these exclusive rights are the rights of reproduction and distribution.[2] It is well settled that an entity infringes on the right of reproduction by making a copy without authorization from the copyright holder. The infringer violates the reproduction by *copying* the work irrespective of whether it's sold or given away. The exclusive right of reproduction is tempered by the fair use doctrine.[3] Notwithstanding the continual and stormy debate surrounding fair use, a strong argument can be made that the unfettered copying of copyrighted works conducted on many of the existing P2P networks falls outside of the fair use concept as elucidated by the Supreme Court in *Sony Corporation of America v. Universal City Studios, Inc.*[4]. It follows then indeed those who "share" are without question, infringing.

The opposition's rhetoric also misses the mark concerning the process by H.R. 5211 will be considered. Indeed, many of the groups and individuals who have registered complaints about H.R. 5211 demonstrate a fundamental misunderstanding of the legislative process. Legislation, especially ones dealing with complex technology issues evolve organically. It is clear the author and co-sponsors of this bill did not intend the bill as introduced to be the final product. Indeed, this hearing is being held to solicit commentary and ideas that will undoubtedly find their way into the bill. It is also inaccurate to suggest that this bill is a legislative "stake in the ground" from which the uber-DRM bill will emerge.

[2] 17 USC 106(1)-(3).
[3] 17 USC 107.
[4] 464 US 417.

1413 K Street, NW * 12th Floor * Washington, DC * Tel: 202-331-2130 * Fax: 202-331-2139 * email: info@ACTonline.org * www.ACTonline.org

2. Why technology self help is a useful mechanism for enforcement

Due in part to the nature of their technology and due in part to the potential for liability exposure, companies that produce anti-piracy technology such as: Overpeer, Vidius, NetPD, Media Defender and MediaForce are reticent to discuss aspects of their products and enrich the innovation of anti-piracy technology. In response, one major file trading network, Morpheus has plans to implement its own countermeasures in an attempt to foil spoofing technology.[5] One major benefit of H.R. 5211 is that it will create an "arms-race" environment whereby any number of companies can seek to provide anti-piracy tools to copyright owners.

Another argument in favor of deploying technology to enforce copyright is that it's far more effective than bringing individual lawsuits against infringers. Tools that allow for widespread spoofing and interdiction are in the best position to effectuate the goal reducing copyright infringement by frustrating would be pirates. Limited amounts of spoofing, redirection and decoying of infringing works is already occurring on a number of P2P networks. There is evidence that the result has been some reduction in the amount of sharing as users become discouraged by downloading less than quality content. It stands to reason that the development and extensive implementation of tools could create sufficient doubt as to the quality of content on the current P2P networks as to create a flight to any number of legitimate distribution models. By contrast, a litany of lawsuits would only create user animosity while allowing infringers to continue their illicit behavior while the case is adjudicated.

3. Specific technology related issues

a. Denial of Service (DoS) Attacks

Many commentators have suggested that the only practical remedy available to copyright holders will be DoS attacks. These DoS will take the form of repeated downloads of a file from the PCs where the file is resident. The result would be a significant impediment of the file's availability for download. Arguably, one ancillary effect would be the slowdown of the entire P2P network, including the distribution of authorized content. However, pursuant to 514(c), the copyright holder must notify the Department of Justice the "specific technologies" they intend to use. This provision also requires the Attorney General to specify what shall be in the notice. It seems only logical that the Attorney General would require that the copyright holder explain what, if any, collateral damage would follow from any tool and seek to encourage use of technologies that would effectuate the goal of the bill with less "blunt force trauma."

Moreover, arguments against the use of DoS based upon the burden it would place on the exchange of legitimate content are not persuasive. While there may be some slowdown in the ability to exchange all types of content, as the number of unauthorized content traders dwindles, it follows that the DoS incidents will decrease and traffic speed will increase.

[5] See, "Music industry swamps swap networks with phony files," San Jose Mercury News, June 27, 2002. http://www.siliconvalley.com/mld/siliconvalley/3560365.htm.

1413 K Street, NW * 12th Floor * Washington, DC * Tel: 202-331-2130 * Fax: 202-331-2139 * email: info@ACTonline.org * www.ACTonline.org

b. Destruction of peer to peer networks.

Some have raised the notion that the actions taken to 512(a) will mean the end of P2P networks. Indeed, the deployment of anti-infringement technologies may destroy P2P networks that are designed primarily to share unauthorized content. Then again, isn't that the point?

It is no secret that P2P networks are undergoing a migration away from the Napster model to a legitimate distributed enterprise computing model. Indeed some commentators have noted that the P2P architecture will play a significant role in the emergence of Web services. A key component of this "renaissance" will be the quality of service of the P2P networks. Therefore, efforts to identify and eradicate elements that degrade this quality should be promoted.

c. Instant messaging

One unintended consequence that was addressed in the language of the bill, but that may still arise is the disruption of an application not designed to share files but that has the potential to do so. For example, there are a number of collaboration and messaging applications, including some server-less versions, which can be used to share files. If a significant number of users start using the collaboration or messaging software for the purpose of illegal file sharing, it is conceivable that the content owner would act to disable the collaboration or messaging software entirely. Though not consistent with the intent of the legislation, the content owner's action could have a negative effect on the development of this platform. Again, because this bill is being vetted publicly, it is likely that subsequent interpretation of the bill language may address this scenario.

4. Enhancements to H.R. 5211

H.R. 5211 is a solid attempt to address a serious problem. To move all parties towards the goals of curtailing piracy while stimulating the growth of the P2P platform as a distribution model, it is critical that this bill accurately balance the rights of copyright holders and the interest of users. To that end we recommend the following enhancements to H.R. 5211.

A large percentage of those who trade infringing content on P2P networks are teenagers, college students and others who are trading a small number of unauthorized works. It is logical to assume that many of these users could be persuaded to voluntarily abandon the network if given a notification of the potential consequences posed under this bill and the Digital Millennium Copyright Act (DMCA). This notification could take the form of a small data file explaining that illegal content was found in a public accessible P2P folder and that it should be removed. This would not only further the goal of reducing the amount illegal content trading, but also minimize the need for interdiction of or other impairment. This notice should be integrated into section 514(a).

One of the significant concerns raised by the opponents of H.R. 5211 is that those persons whose computers have been the subject of the self-help measures will not know it. In scenarios where the computer has been wrongly targeted or the effects of the content owner' self-help technologies are beyond those allowed by this bill, the computer owner may not know the cause of his or her computer

1413 K Street, NW * 12th Floor * Washington, DC * Tel: 202-331-2130 * Fax: 202-331-2139 * email: info@ACTonline.org * www.ACTonline.org

problems. To remedy this concern, content owners should notify all users on which these technologies have been implemented either electronically or by mail via through their ISP.

Copyright holders should give notification of the specific IP addresses to the Department of Justice in addition to the notification of technologies they must give under section 514(c)(1)(A). The notification could take the form of a report of IP addresses and the illegal content found. This practice of compiling lists of IP address currently conducted pursuant to the DMCA notice requirement.[6] This notification, also protected under the FOIA exemption under 512(g), would provide a record that could not be altered by copyright holder. This would be particularly important in the event of a failure of impairment technology that removes the rights holder from the 514(a) safe harbor.

The phrase "unauthorized distribution" should be changed to "illegal distribution." The term "unauthorized" is confusing given the ongoing debate surrounding fair use. It seems obvious that if material is placed into a public folder which carries a name specific to a P2P network, it is there to be shared with all users as part of the network's commercial nature and is therefore an infringement.[7] Thus, the law will allow content owners to prevent distribution that is "illegal" under copyright law, but the safe harbor will not extend to actions taken against distribution that falls within the legally gray area between the illegal and authorized.

Conclusion

Once the rhetorical dust clears, we can see that copyright holders have a legitimate interest in protecting their content and one which is not adequately served in the current environment. The specious apocalyptic predictions of the CCIA on behalf of Morpheus, a business built on illegal file trading, need to be set aside in favor of a more balanced view. There are significant ways to improve this legislation to ensure compliance by copyright holders but it is clear that H.R. 5211 is on the right track. Why *else* would Morpheus be barking so loudly?

[6] See 17 USC 512(c)(3)(A). This section requires that effective notification include "information sufficient to allow the service provider to locate [infringing] material."
[7] For example, the P2P network KaZaA uses a public folder entitled "My Shared Folder."

1413 K Street, NW * 12th Floor * Washington, DC * Tel: 202-331-2130 * Fax: 202-331-2139 * email: info@ACTonline.org * www.ACTonline.org

PREPARED STATEMENT OF EDWARD W. FELTEN

To the Distinguished Members of the Subcommittee on Courts, the Internet, and Intellectual Property:

I am writing to provide an independent perspective on some technical issues raised by Congressman Berman's proposed "P2P Piracy Prevention Act" (the "Berman Bill"). I offer this testimony in the hope that it will help the Subcommittee better understand the technical effects of the Berman Bill.

I write as an expert on computer security. I am an Associate Professor of Computer Science at Princeton University, and Director of Princeton's Secure Internet Programming Laboratory. I have published more than fifty research papers and two books, and my research has been covered widely in the national press. In addition to my service on corporate advisory boards, I serve on the Information Science and Technology (ISAT) advisory board of the Defense Advanced Research Projects Agency. I am co-chair of an ISAT study on "Reconciling Security with Privacy," and am a member of the National Research Council's study group on "Fundamentals of Computer Science." I have also served as the primary computer science expert witness for the Department of Justice (DOJ) in the Microsoft antitrust case, and as a technical advisor to the DOJ's Antitrust Division under both the Clinton and Bush administrations.

I share the Subcommittee's condemnation of widespread on-line copyright infringement. I support both legal action against copyright infringers, and technical self-help by copyright owners within the bounds of current law. The issue is not whether copyrights should be honored, nor whether the Berman Bill is well-intentioned, but rather what effect the bill would have.

I would like to bring two things to the Subcommittee's attention.

First, the Berman Bill's definition of "peer-to-peer" may be problematic. Peer-to-peer networking is not a new phenomenon, but has been the dominant mode of operation since the very beginning of the Internet. The World Wide Web itself is a peer-to-peer file sharing system, as the term "peer-to-peer" is commonly understood. More to the point, the Web clearly meets the Berman Bill's definition of "publicly accessible peer-to-peer file trading network." Therefore, *the bill, as written, flatly authorizes "self-help" attacks on the World Wide Web, and not just on users of file-trading networks like KaZaa and Gnutella.*

It seems difficult to redraft the bill to carve out the Web and other legitimate network services, without creating an escape hatch for the types of peer-to-peer networks that the bill's supporters would like to see covered. The reason for this difficulty is simple: there is really little difference at a technical level between the Web and peer-to-peer systems like KaZaa and Gnutella. The difference between these systems is not so much in how they are designed, but rather in what their users do with them.

(I also note in passing that the bill's exception for systems that "route all . . . inquiries or searches through a designated, central computer" may not have the effect that the bill's drafters envisioned. Nowadays large sites do not use a single "designated, central computer," but instead use a group of computers which cooperate to serve users' requests. It would appear, therefore, that the bill's "designated, central computer" exception would cover few if any of the large central sites for which the exception appears to be intended.)

Second, there is reason to doubt the efficacy of the technical measures that copyright owners want to use.

The copyright owners' representatives who testified in person at the Subcommittee's hearing could identify only one technical measure they plan to employ if the Berman Bill is enacted. This measure, which they call "Interdiction," was described in the written and oral testimony of Mr. Randy Saaf. Based on Mr. Saaf's description, "Interdiction" is apparently just a new name for a well-known type of denial of service attack.[1]

A "denial of service attack" is a hostile action that exhausts the resources of a system or program, so that that system or program cannot operate, or can operate only in a degraded fashion. Some denial of service attacks seek to overwhelm a target computer's Internet connection with traffic, while others seeks to exhaust some other resource that the target needs.

For example, the so-called "SYN flood" denial of service attacks that (temporarily) disabled CNN, eBay, Yahoo!, and Amazon, in February 2000, disabled the target systems by initiating network connections with the targets in such a way that the

[1] For example, a speaker at this year's H2K2 "Hackers on Planet Earth" conference reportedly suggested using the attack that Mr. Saaf calls "Interdiction" against governmental and institutional Internet sites as a form of "online demonstration."

targets were no longer able to accept further connections. Though the targets had plenty of spare communication bandwidth available, that bandwidth did them no good since they could not accept any more incoming network connections.

"Interdiction" operates on a similar principle. According to Mr. Saaf's written testimony:

> MediaDefender's computers hook up to the person using the P2P protocol being targeted and download the pirated file at a throttled down speed. MediaDefender's computers just try to sit on the other computers' uploading connections as long as possible, using as little bandwidth as possible to prevent others from downloading the pirated content. . . .
>
> The goal is not to absorb all of that user's bandwidth but block connections to potential downloaders. If the P2P program allows ten connections and MediaDefender fills nine, we are blocking 90% of illegal uploading.

At present, Interdiction attacks apparently deny service only to the peer-to-peer program running on a user's computer, and not to any other programs. The designers of peer-to-peer software will not simply accept this situation, but will respond by modifying their software to thwart such targeted denial of service attacks. They might do this, for example, by eliminating the self-imposed limit on the number of connections the peer-to-peer program will accept. These countermeasures will start an "arms race" between copyright owners and peer-to-peer system designers, with copyright owners devising new types of targeted denial of service attacks, and peer-to-peer designers revising their software to dodge these targeted attacks.

Computer security analysis can often predict the result of such technical arms races. For example, analysis of the arms race between virus writers and antivirus companies leads to the prediction that antivirus products will be able to cope almost perfectly with known virus strains but will be largely helpless against novel viruses. This is indeed what we observe.

A similar analysis can be applied to the arms race, under the Berman Bill's rules, between peer-to-peer authors and copyright owners. In my view, the peer-to-peer authors have a natural advantage in this arms race, and they will be able to stay a step ahead of the copyright owners.[2] Copyright owners will be forced either to give up on the strategy of narrowly targeted denial of service attacks, or to escalate to a more severe form of denial of service, such as one that crashes the target computer or jams completely its Internet connection. I understand that these more severe attacks are currently illegal, and would not be legalized by the Berman Bill, so such an escalation would not be possible within the law even if the Berman Bill is enacted. I conclude that the Berman Bill as written is unlikely to do copyright holders much good in the end.

[2] I understand that the House of Representatives uses technical means to prevent peer-to-peer file trading by its employees. Of course, the ability of an organization such as the House to control the use of its own systems does not imply that copyright owners can exert the same level of control on others' systems.