PEER-TO-PEER PIRACY ON UNIVERSITY CAMPUSES

HEARING

BEFORE THE

SUBCOMMITTEE ON COURTS, THE INTERNET,
AND INTELLECTUAL PROPERTY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

FEBRUARY 26, 2003

Serial No. 2

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

85–286 PDF WASHINGTON : 2003

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
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
JOHN R. CARTER, Texas
TOM FEENEY, Florida
MARSHA BLACKBURN, Tennessee

JOHN CONYERS, Jr., Michigan
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
LINDA T. SÁNCHEZ, California

Philip G. Kiko, *Chief of Staff-General Counsel*
Perry H. Apelbaum, *Minority Chief Counsel*

Subcommittee on Courts, the Internet, and Intellectual Property

LAMAR SMITH, Texas, *Chairman*

HENRY J. HYDE, Illinois
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
WILLIAM L. JENKINS, Tennessee
SPENCER BACHUS, Alabama
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
JOHN R. CARTER, Texas

HOWARD L. BERMAN, California
JOHN CONYERS, Jr., Michigan
RICK BOUCHER, Virginia
ZOE LOFGREN, California
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
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

FEBRUARY 26, 2003

OPENING STATEMENT

WITNESSES

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

PEER-TO-PEER PIRACY ON UNIVERSITY CAMPUSES

WEDNESDAY, FEBRUARY 26, 2003

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

The Subcommittee met, pursuant to call, at 10:05 a.m., in Room 2141, Rayburn House Office Building, Hon. Lamar Smith [Chairman of the Subcommittee] presiding.

Mr. SMITH. The Subcommittee on Courts, the Internet, and Intellectual Property will come to order.

I am going to recognize Members for opening statements, and then we will proceed as quickly as we can to hear from our witnesses. And I will recognize myself first for an opening statement.

"The Congress shall have power to promote the progress of science and useful arts by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." Those words, of course, are from the United States Constitution, Article 1, Section 8.

The wisdom of our Country's Founders still rings true today. The authors of the Constitution understood that the incentive to create would greatly benefit the public. And more than two centuries after the fact, our lives have been enriched as a result—with inventions and products to make our lives easier, and music and movies to lift our spirits.

Following in the steps of the previous Chairman of the Subcommittee, Howard Coble, it is my hope that our work over the course of this Congress will help boost the economy, increase productivity, and improve the quality of life for all Americans.

At the outset, let me say that I am pleased to be associated with the Ranking Member, Howard Berman. We have served as Chairman and Ranking Member before on another Committee, and I like that particular configuration. Mr. Berman is thoughtful, knowledgeable, and an effective Member of Congress. And I look forward to his contributions as we tackle the difficult and complex issues surrounding intellectual property law.

Let me also welcome the other Members of the Subcommittee. I know this Subcommittee is a priority to you all, and I look forward to your involvement as well.

Today, the Subcommittee will conduct an oversight hearing on peer-to-peer piracy on university campuses. The rise of the Internet and new digital media have changed the way the public enjoys entertainment products. One of the advantages of digital formats is that they offer extremely high-quality reproduction of audio and video. A major disadvantage is that digital formats make the works very susceptible to piracy since every digital copy offers a perfect reproduction.

The problem is only exacerbated by peer-to-peer file-sharing networks. While P2P technology has many benefits, it also permits the widespread and massive distribution of digital music, movies, and software files, which often results in copyright infringement. Industry officials estimate that there are billions of illegal files downloaded every week. The result is lost sales to businesses and lost royalties to artists and copyright owners.

The ready access to the file-sharing sites and the ease with which files can be downloaded by broadband connections has emboldened American university students to engage in piracy. This is a serious problem that undermines the protections provided by the Constitution.

Some staggering statistics illustrate the magnitude of the problem. Research of FastTrack, a peer-to-peer file-sharing service, showed that 16 percent of all the files available at any given moment are located at IP addresses managed by U.S. educational institutions. In addition, FastTrack users trading from networks managed by U.S. educational institutions account for 10 percent of all users on FastTrack at any given moment. It's very unlikely that this amount of file-sharing activity is in furtherance of class assignments.

In an effort to curb university-based piracy, content owners and educational associations formed the Joint Committee of Higher Education and Content Communities, which will meet periodically to address student piracy issues.

This hearing will focus on the extent of peer-to-peer piracy on university campuses and what measures content owners and universities are taking to address the problem.

Mr. SMITH. We look forward to hearing from the witnesses today, and the Ranking Member, Mr. Berman of California, is recognized for his opening statement.

Mr. BERMAN. Well, thank you very much, Mr. Chairman.

I have real enthusiasm for working with you in your new chairmanship of this Subcommittee. You mentioned you liked the configuration of Chair and Ranking Member. My recollection of the last time we were Chair and Ranking Member, we had equal numbers of each party on the Committee on which we were Chair and Ranking Member, and I liked that configuration. [Laughter.]

Mr. SMITH. That was the Ethics Committee, as I recall, is that right?

Mr. BERMAN. I liked the configuration. I didn't say I liked the Committee. [Laughter.]

In any event, you have chosen for this hearing an important issue for your first hearing as Chairman of this Subcommittee, and I think it is a good sign that you will focus the Subcommittee on both interesting and relevant issues during your tenure.

Copyright piracy on P2P networks like KaZaA and Morpheus is a huge problem. P2P networks are responsible for approximately 2.5 billion downloads per month. On FastTrack-based P2P networks alone, an estimated 3 million to 5 million computers are making between 700 million and 900 million files available for download at any given moment.

There is no doubt that the vast majority of these P2P uploads and downloads constitutes copyright infringement. Music, movie, and television programs constitute an estimated 89 percent of the files on P2P networks. As the 9th Circuit clearly held in the Napster case, the unauthorized distribution and reproduction of copyrighted works by total strangers through a public P2P network is copyright infringement, pure and simple.

As the 9th Circuit also held, no colorable claim of fair use excuses these infringements. The attempt to make such an excuse not only ignores the reality of the theft but is an insult to creators. It is the copyright owner's right, not a pirate's, to choose whether to distribute a copyrighted work through a P2P system. If the copyright owner wants to use P2P to distribute his work, that's great. If not, the owner has a right to refuse.

The argument about the propriety of illegal P2P file trafficking should end there. But some try to further excuse this theft. They make patronizing assertions that copyright owners actually benefit from this massive theft and thus should welcome the usurpation of their property rights.

The truth, of course, is that the P2P file trafficking causes great harm to copyright owners. General economic indicators show the extent of harm. Revenues from sales of music CDs plummeted 20 percent over 2001 and 2002, and the sales numbers for January 2003 indicate more of the same. These sales declines cannot be explained away as reflections of the general economic downturn from 2000 to the present.

Economist Harold Vogel has charted a rapid decline in unit sales of CDs since 1999, well before the economic turndown, and notes that this decline corresponds directly with the introduction of Napster.

The impact on individual creators is also great. Each illegal P2P download of a copyrighted song robs a songwriter of 8 cents. Those 8 cents multiplied by the billions of P2P downloads would mean a new life for the vast majority of songwriters who earn less than $20,000 in royalties per year. Similarly, illegal P2P downloads of television programs destroy the syndication market upon which the hopes of many directors, writers, and actors hinge.

Unfortunately, colleges play a prominent role in contributing to P2P piracy. A recent study showed that 16 percent of all the files available at any given moment on the FastTrack network are located at IP addresses managed by U.S. educational institutions. This means that educational institutions are offering between 111 million and 142 million mostly infringing files to the universe of P2P users at any given time.

It is imperative that colleges work with copyright owners to stem the flood of P2P piracy through their computer networks. As Jack Valenti pointed out in a recent speech at Duke University, colleges are in the business of creating upstanding citizens who will respect the American moral compact. To create such citizens, colleges must teach by example, and that example can't be adherence to the credo of "Do it, if you can get away with it."

Furthermore, colleges can't expect Congress to continuously help them on intellectual property issues if they do not act as responsible members of the intellectual property system. From laws facilitating technology transfer to those enabling distance education, Congress has willingly helped colleges protect or use intellectual property.

As with the collaborative research legislation we may take up later this year, I expect that Congress will continue to provide such assistance. But the willingness of Congress to address these issues will wane if colleges ignore the massive P2P piracy occurring on their systems.

Moreover, their own self-interest dictates that colleges take action to deal with P2P piracy. Bandwidth, security, and privacy concerns really require colleges to get the problem in hand. It consumes an enormous amount of college bandwidth, P2P piracy, and as a result, increases bandwidth cost while draining the resources available for research and academic pursuits.

Security concerns should also lead colleges to stop P2P piracy through their networks. As Professor John Hale will testify, FastTrack and Gnutella, the two most popular P2P protocols, enable the transfers of viruses, the implanting of malicious computer programs like spyware, and tunneling through network firewalls and filters.

Concerns regarding the privacy implications of P2P networks are also quite real. As documented in the white paper submitted by Professor Hale and in a separate study by Hewlett-Packard, P2P network users often expose their most private information and correspondences to the whole P2P network. Unwittingly, P2P users frequently allow their credit card numbers, e-mail inboxes, and even tax information to be shared with other P2P users.

Mr. Chairman, I have a few more points to make, but I think I will shorten my opening statement, which has not been so short, and ask for permission to put the whole statement into the record.

Mr. SMITH. Thank you, Mr. Berman. Without objection, your entire statement will be made a part of the record.

[The prepared statement of Mr. Berman follows:]

PREPARED STATEMENT OF THE HONORABLE HOWARD L. BERMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Chairman Smith:

You have chosen an important issue for your first hearing as Chairman of the Subcommittee. It is a good sign that you will focus the Subcommittee on interesting and relevant issues during your tenure.

Copyright piracy on P2P networks like Kazaa and Morpheus is a huge problem. P2P networks are responsible for approximately 2.5 billion downloads per month. On FastTrack-based P2P networks alone, an estimated 3 to 5 million computers are making between 700 and 900 million files available for download at any given moment.

There is no doubt that the vast majority of these P2P uploads and downloads constitute copyright infringement. Music, movie, and television programs constitute an estimated 89% of the files on P2P networks. As the 9th Circuit clearly held in the Napster case, the unauthorized distribution and reproduction of copyrighted works by total strangers through a public P2P network is copyright infringement pure and simple.

As the 9th Circuit also held, no colorable claim of fair use excuses these infringements. The attempt to make such an excuse not only ignores the reality of the theft, but is an insult to creators. It is the copyright owner's right, not a pirate's, to choose whether to distribute a copyrighted work through a P2P system. If the copyright owner wants to use P2P to distribute his work, that's great. If not, the owner has the right to refuse.

The argument about the propriety of illegal P2P file trafficking should end there, but some try to further excuse this theft. They make patronizing assertions that copyright owners actually benefit from this massive theft, and thus should welcome the usurpation of their property rights.

The truth, of course, is that P2P file trafficking causes great harm to copyright owners. General economic indicators show the extent of harm. Revenues from sales of music CDs plummeted 20% over 2001 and 2002, and the sales numbers for January 2003 indicate more of the same. These sales declines cannot be explained away as reflections of the general economic downturn from 2000 to present. Economist Harold Vogel has charted a rapid decline in unit sales of CDs since 1999—well before the economic downturn—and notes that this decline corresponds directly with the introduction of Napster.

The impact on individual creators is also real. As I have noted before, each illegal P2P download of a copyrighted song robs a songwriter of 8 cents. Those 8 cents multiplied by the billions of P2P downloads would mean a new life for the vast majority of songwriters who earn less than $20,000 in royalties. Similarly, illegal P2P downloads of television programs destroy the syndication market upon which the hopes of so many directors, writers, and actors hinge.

Unfortunately, colleges play a prominent role in contributing to P2P piracy. A recent study showed that "sixteen percent of all the files available at any given moment on the FastTrack network are located at IP addresses managed by U.S. educational institutions." This means that educational institutions are offering between 111 and 142 million mostly-infringing files to the universe of P2P users at any given time.

It is imperative that colleges work with copyright owners to stem the flood of P2P piracy through their computer networks.

As Jack Valenti pointed out in a recent speech at Duke University, colleges are in the business of creating upstanding citizens who will respect the American moral compact. To create such citizens, colleges must teach by example, and that example can't be adherence to the credo of "Do it if you can get away with it."

Furthermore, colleges cannot expect Congress to continuously help them on intellectual property issues if they do not act as responsible members of the intellectual property system. From laws facilitating technology transfer to those enabling distance education, Congress has willingly helped colleges protect or use intellectual property. As with the collaborative research legislation we may take up later this year, I expect that Congress will continue to provide such assistance. However, the willingness of Congress to address these issues will wane if colleges ignore the massive P2P piracy occurring on their systems.

Furthermore, their own self-interest dictates that colleges take action to deal with P2P piracy. Bandwidth, security, and privacy concerns require colleges to get the problem in hand.

P2P piracy consumes an enormous amount of college bandwidth, and as a result, increases bandwidth costs while draining the resources available for research and academic pursuits. 88% of Residence Hall networks at the University of Indiana were at one time consumed with P2P file-trafficking. When Texas Christian University blocked Napster, it freed up 70% of its bandwidth.

Freeing up network bandwidth by blocking illegal P2P file-trafficking has saved colleges significant sums. Kansas State estimated that it saved more than $100,000, or a quarter of its bandwidth costs. In a time of shrinking school budgets, these savings are significant.

Security concerns should also lead colleges to stop P2P piracy through their networks. As Professor John Hale will testify, FastTrack and Gnutella, the two most popular P2P protocols, enable the transfer of viruses, the implanting of malicious computer programs like spyware, and "tunneling" through network firewalls and filters. Once the networks have been breached, sensitive information can be stolen or corrupted, critical university computer systems can be crashed, and university computers can be "enslaved" to carry out Denial of Service attacks. It is these very security concerns that led the House, Senate, and U.S. Courts to disable the use of popular P2P networks on their respective computer systems.

Concerns regarding the privacy implications of P2P networks are also quite real. As documented in the White Paper submitted by Professor Hale and in a separate study by Hewlett-Packard, P2P network users often expose their most private information and correspondences to the whole P2P network. Unwittingly, P2P users frequently allow their credit card numbers, email inboxes, and even tax information to be shared with other P2P users.

Piracy apologists like to argue that stopping P2P piracy somehow impinges on the privacy of file-traffickers. As the Hale and H-P studies show, it is participation in file-trafficking itself threatens the privacy of file-traffickers. Thus, colleges concerned with the privacy of their students and other members of the college community should act to stop P2P piracy, not allow it to flourish.

I understand that I may be preaching to the choir here. The schools represented by our witnesses today have all taken dramatic steps to stop P2P piracy from occurring on their networks. Your schools, and you yourselves, are to be commended for acting in enlightened self-interest. Rather than preaching to you, I mean to encourage other colleges to follow your lead.

I am heartened to hear that a group of colleges are meeting with copyright owners to discuss ways to address P2P piracy on campus. In particular, I am most interested in your efforts to craft a model policy for best practices that colleges should adopt to address P2P piracy. Widespread adoption of such best practices, and the self-regulation model they represent, is far preferable to a legislative mandate of such standards.

It seems critical that you develop this best practices model with all speed, so that colleges across the country can implement them before the P2P piracy problem spirals further out of control. I hope you will keep this Subcommittee appraised of your progress in this area, and of subsequent progress with implementation.

Thank you, Mr. Chairman, and I yield back the balance of my time.

Mr. SMITH. And let me say to the other Members, normally I'd encourage you to make opening statements a part of the record. But this being our first hearing, and I know several Members have constituents in the office, I'll be happy to recognize Members for brief opening statements, if they have them.

I know the gentleman from Florida, Mr. Keller, has an opening statement, and he'll be recognized now.

Mr. KELLER. Thank you, Mr. Chairman.

Mr. Chairman, if a student walks into a campus bookstore and puts a sweatshirt in his backpack, everybody knows what to call it. It's shoplifting. If that same student goes into the same store and sticks a CD or a DVD in the same backpack and walks out, it, too, is shoplifting. The school has disciplinary policies and pursues them, as they would with any other crime.

There is no difference if the student takes that same music or movie by downloading it off the Internet while sitting in the dorm. Colleges and universities have a duty to address these crimes aggressively. School presidents and other administrators cannot stand by as taxpayer-funded information systems and tuition dollars are being used to build Internet systems that help facilitate unethical behavior.

Now, that may sound hokey to some people. But schools have an important role in shaping America's future leaders. The fact is that no professor can address the ethical transgressions we have read about in the business community if his students go back to the dorm and commit crimes of their own. There must be a clear and consistent message.

Some students may feel that downloading music and movies is victimless. In fact, the theft on college campuses is rampant and widespread and undermining one of America's most important industries. Some students may feel that they can steal anonymously. It is noteworthy that we now have the ability to track those who are committing online crimes.

I read a recent article citing a Kent State University administrator who claimed that 40 percent of the university's bandwidth was being consumed by 10 students. An article about Cornell University's problems stated that over 50 percent of their Internet network bandwidth was for KaZaA, and two-thirds of the KaZaA traffic was outbound, meaning that Cornell was actually facilitating theft by people from outside the university. Cornell found that the heaviest bandwidth user was using 2,800 times the bandwidth of the typical user.

Mr. Chairman, I commend you for focusing attention on this very troubling situation, and I look forward to working with Dr. Spanier and other educational leaders to help find solutions that do not disrupt the ability of the university Internet systems to fulfill their rightful and lawful education missions.

I yield back.

Mr. SMITH. Thank you, Mr. Keller. The gentlewoman from California, Ms. Lofgren, is recognized for an opening statement.

Ms. LOFGREN. Thank you, Mr. Chairman.

I look forward to the testimony today and to the future hearings on the issue of copyright and technology. Clearly, we have massive infringement going on in P2P networks, and that is a concern. I mean, there is no question that that is problematic.

I am pleased to see that the education community is not simply looking at legislation, but looking to themselves to see what they might do to be responsible about this issue. And my friend Dr. John Hennessy is heading up the education best practices task force. I am hopeful that that will be a very positive step for our Country.

However, I also note that it is, I'd say, unlikely in the extreme that P2P networks will be eliminated. And in fact, it's behavior and student behavior that needs to be changed so that infringement does not continue to occur. Clearly, there are non-infringing uses as well to P2P networks, and so universities will tread with some caution, I think, on what they do vis-a-vis their students.

I am hopeful also that we will hear, if not today, in future hearings, what efforts are being made to meet the consumer demand for content online because that is about human behavior also. The fact that that content interest has not yet been met does not excuse infringement, but it is part of the whole behavior situation that we need to take a look at. And I am hopeful that as the months go on that we will also have an opportunity to look at that.

And with that, I will not delay the witnesses further, and I yield back. Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Ms. Lofgren.

Are there other Members who wish to make opening statements? Does the gentleman from Florida, Mr. Wexler, have an opening statement? He is recognized.

Mr. WEXLER. Thank you, Mr. Chairman. And I want to echo Mr. Berman's comments in terms of our looking forward to working with you as the Chairman. And I know you have a deep interest in these issues and a very fair interest in the past, and it's very exciting for those of us on the Committee.

I would just like to say a few words, if I could, in terms of the issue before us today and the issue specifically with respect to universities. I find it deeply troubling that intellectual property protections are most in danger at our country's universities, which have long been a significant source for intellectual property in this country.

But I have come to understand, even as American colleges and universities vigorously protect the intellectual property of their scientists, their professors, and their legal scholars, the property of artists and musicians are being widely traded on university network servers with few consequences, at least until very recently.

At almost any time of the day or night, students are sharing, stealing, and downloading songs and movies with easily accessible technology on high-speed university networks. However easy this file-stealing has become, it is far from justifiable. It is electronic theft, plain and simple. And it is on a path to cripple American artists, large and small.

Universities have always been the strongest bases of support for independent music. I'm very concerned that file-sharing, which is financially devastating to the entertainment industry, will have the unintended effect of killing this kind of small, experimental music. For we all know that it is not just the guaranteed successes that are most hurt by this theft. It is small musicians, songwriters, and artists who will have to find other work if electronic theft continues as it has at universities and in the larger Internet community.

Of course, all stealing is equally reprehensible, but the marginal effect of this theft is far more destructive for the smaller, less mainstream artists. I would like to quickly bring to the attention of the Subcommittee one example of exactly what we would lose if this rampant file-stealing continues.

Since she rose from relative obscurity to win every Grammy for which she was nominated last week, Norah Jones expressed her creativity and originality and was justly recognized. Sadly, she is exactly the kind of artist who might not be heard if this music piracy continues.

Musicians like Bruce Springsteen and Eminem will certainly be hurt by piracy but are essentially guaranteed—virtual guaranteed successes, and they can count on having their songs produced and marketed.

But if piracy continues to hurt the music industry, companies will no longer be able to take risks with more innovative and cutting-edge artists as they did with Ms. Jones, and we will all be the poorer for it.

Congress's responsibility is to maintain strong copyright protection laws in order to foster creativity and encourage investment. I am by no means suggesting censorship, violating the privacy of individuals, or the dampening of academic debate.

American universities have been an invaluable source of innovation and debate for this country. This is why I am concerned with the effect bandwidth caps and other anti-piracy measures might have on legitimate academic research and free speech at universities. And I hope these concerns, I'm sure they will, will be addressed by today's witnesses.

While the network restrictions might discourage students from breaking the law, they may also hinder legitimate exchanges, and it is clear that no simple universal solution will end Internet piracy. I hope, however, it's equally clear that peer-to-peer piracy cannot be allowed to continue, particularly in a setting that purports to teach our children respect for law and American values of fairness.

I want to thank President Spanier and President Broad for being here today, and I look forward to hearing more regarding their experiences combating this problem.

As we continue to hear testimony on this important intellectual property issue, we all must keep in mind that the overwhelming majority of P2P transfers are of copyrighted materials.

These transfers are theft. There can be no justifying or excusing them, and it is the duty of Congress to protect these properties on university campuses and throughout the world.

Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Wexler.

Are there other Members who wish to be recognized? The gentleman from New York, Mr. Weiner?

Mr. WEINER. Thank you, Mr. Chairman. I'll be brief. And I, too, look forward to your chairmanship of this Committee.

You know, this is that rare issue that there is virtual consensus on the panel and, frankly, probably in Congress that something needs to be done to address the problem. Yet we on this Committee and, frankly, we in this Congress have always been very responsive when all sides have said, you know what, just wait.

This, like many other aspects of the Internet, is a place where we have been encouraged to avoid legislating problems because, frankly, technology has often outstripped the problems and outstripped the solutions at once.

We've been told on several occasions that the problem of P2P copyright violations and illegal sharing requires a technical solution or, in some cases, might require a public relations solution. Although I would have liked that guy from Limp Bizkit to be in "agreeance" on fixing this problem rather than the other thing he was addressing.

But we are reaching, I would say, the end of our ropes here. I think that there is consensus that has emerged that, you know what, we're going to wait for so long. And while I think all sides of this debate is to let us try to work it out, I think the fact that we're having another hearing on this, the fact that Members of Congress have said in, as I said, virtual unanimity that something needs to be done should be a message to all of those who will testify today and those in the industry as well that, you know, we are reaching that point that, on a bipartisan level, that we want to act to stop this illegal activity.

So I would hope that in the testimony we hear today, we don't hear the same refrain that we've heard before, which is sometimes, yes, we've got a problem, but Congress should step back. I'd like to be hearing today how long it's going to be, as these technological solutions are worked out, how long it's going to be before the public relations campaign kicks in.

Because every day constituents of mine in New York City, which is a breadbasket for creative activity, people are losing money, losing careers, and these are not the Britney Spears of the world. These are the people who help Britney Spears write her—I guess they're called songs. [Laughter.]

These are people who are, you know, $20,000, $30,000 a year creative artists that are being denied their living because of this problem.

But I thank you, Mr. Chairman, for addressing this so early in the session, and I hope it's just the first step in what will be others.

Mr. SMITH. Thank you, Mr. Weiner.

And let me thank all the Members who are here for their attendance. We may actually be setting some kind of a record for a hearing, and I hope this kind of attendance continues as well.

Also, let me thank those of you who are in the audience today. There is clearly a high level of interest in the subject at hand, and we appreciate your being here as well.

A couple of housekeeping matters. First of all, all witnesses' statements will be made a part of the record, as will the speech by Jack Valenti at Duke University. And also let me say that we intend to enforce the 5-minute rule. So we hope you can conclude your testimony in 5 minutes. If not, perhaps you will have time to finish it during the question and answer period as well. And we'll hold Members to 5 minutes, too.

Let me introduce our witnesses today. Our first witness is Hilary Rosen, chairman and chief executive officer of the Recording Industry Association of America, the trade group representing the U.S. sound recording industry. She was named president and CEO of the RIAA in January 1998 after more than 11 years of service to the organization. Ms. Rosen holds a bachelor's degree in international business from George Washington University.

Our next witness is Graham Spanier, president of the Pennsylvania State University and co-chair of the Joint Committee of Higher Education and Content Communities. A distinguished researcher and scholar, he has authored more than 100 publications, including 10 books. He earned his Ph.D. in sociology from Northwestern University, where he was a Woodrow Wilson Fellow, and his bachelor's and master's degrees are from Iowa State University.

And the next witness is Robyn Render, vice president for information resources and chief information officer for the University of North Carolina. Ms. Render serves as the primary adviser to the university president on information technology. Ms. Render holds associate and bachelor's degrees in information systems from the University of Cincinnati.

Our last witness is Dr. John Hale, assistant professor of computer science and director of the Center for Information Security at the University of Tulsa. Dr. Hale has significant expertise in computer security, programming languages, and distributed systems. He has published approximately 40 reference articles and one book. He received the prestigious 2000 National Science Foundation award for his research and educational contributions in the field of computer security.

Welcome to you all. As I say, your statements will be made a part of the record. We look forward to hearing from you, and we will begin with Ms. Rosen.

STATEMENT OF HILARY ROSEN, CHAIRMAN AND CEO, RECORDING INDUSTRY ASSOCIATION OF AMERICA

Ms. ROSEN. Thank you, Mr. Chairman. Good morning, Congressman Berman, other Members of the Committee.

Allow me, Mr. Chairman, to add my congratulations to you as you take on the role of Subcommittee Chairman and pledge the recording industry's cooperation as you go forward on this important work.

And thank you also for your interest in this issue. I think your work with the University of Texas has been extremely constructive and in large part has resulted in some of the working relationships that you'll see demonstrated here today between all of us in the university community.

This hearing could not have come at a better time, for several reasons. The problem of P2P piracy in general is at an all-time high for the music community. And while they were a long time in coming, legitimate music services have arrived and are being extremely well received, eliminating any possible excuse that some may have for engaging in such wholesale piracy.

And importantly, the unique aspects of universities, given their mission and their operations, make the cooperative working relationship that you will see demonstrated here today possible, and it's a welcome model for problem-solving in this area.

I think by now Members of this Committee have seen a demonstration of peer-to-peer networks and witnessed the fact that a majority of the use on them is massive unauthorized distribution of copyrighted works.

That's not to say that the technology itself is bad. There are certainly multiple legitimate uses for P2P, and hopefully, in the future they will be used.

But the people who run these networks now are aggressively exploiting other people's property to support their global criminal activity.

While it's true that many users don't understand the legalities of their behavior, many others do. And it's also clear that the operators of these services well know that they're operating an illegal network. That's why we have to chase them around the globe and why they find criminal havens like Vanuatu so appealing for their corporate headquarters.

Caught up in this illegal practice are the thousands of colleges and universities whose generous provision of large bandwidth to their students, for scholarly and research purposes have resulted in their systems being used as a major supporter of these illegal activities. And a new practice outlined in my testimony, whereby students are actually setting up their own networks using the university capacity, is extremely troubling.

We are very gratified that the leadership of the university community, personified here by the presence of Dr. Spanier, has recognized these problems as mutual and are working with others in the copyright community toward solutions.

It's obvious why we care about this practice. It may not be as obvious why the universities should care. But as you'll hear, their networks are clogged and their bandwidth costs are skyrocketing mostly from people outside their system using the bandwidth to steal music and movies that are residing on students' computers. Students are breaking the law, and universities know they have an obligation to try and educate them and protect them from such activity.

There are other reasons as well. Many people believe, as I do and as Members here have said, that it's simply morally wrong to condone the stealing of other people's property. And Members today have been more eloquent than I could be on this issue. So what's the public interest here?

Of course, Congress wants our young people to evolve into upstanding young adults, but there are other things that you must consider. Many universities and colleges receive Federal and State taxpayer monies. So you have a fiduciary interest if their costs increase due to piracy.

And there are serious threats to people who open up their computer to these networks. Open hard drives facilitate access to significant personal data and risk additional crimes like identity theft. The networks are also used for numerous commercial exploits, such as pornography being pushed to users.

The reduction of sales in the music industry has resulted in far fewer new artist signings over this past year, meaning frankly that the diversity of culture is waning. If bad policies from important institutions result in less music and movies and software being developed, society at large is worse off.

And of course, the protection of intellectual property is in the national interest. During these times of record trade deficits, intellectual property is one of the very few industries that return a favorable balance of trade to the U.S. economy. Protecting that advantage has always been a key mission of this Subcommittee, and its leadership here is well known.

So in recognizing these issues, we are working with the university leadership. I think Dr. Spanier will elaborate some more on how this Committee is working.

My colleague Cary Sherman, RIAA's president, is the co-chair of that Committee with Dr. Spanier. Mr. Sherman is here with me today.

We're extremely hopeful about the potential for this working relationship, and we're certainly impressed with the seriousness with which it's being taken. Our goals are simple. We want to find ways to help the universities take this problem into their own hands by implementing a series of best practices recommendations, which we hope will be developed within the next few months.

Policy recommendations and technical recommendations may be the results of our efforts. We have pledged to explore both. Certainly, these will only be voluntary recommendations, and nothing we do will force universities to adhere to new practices.

Nonetheless, our joint Committee has fine leadership and sincere commitment. We're confident that the results of our work could be an effective model leading all schools on a path that's mutually beneficial, and we look forward to working with this Committee as we proceed on this effort over the next coming months.

Thank you.

[The prepared statement of Ms. Rosen follows:]

Prepared Statement of Hilary Rosen

Mr. Chairman, Congressman Berman, Members of the Subcommittee, I greatly appreciate your inviting me to speak with you on the timely subject of unauthorized peer to peer (P2P) file sharing on university and college computer networks.

Over the years, our industry has benefitted from the emergence of various new technologies. The evolution from wax cylinders to vinyl, from vinyl LPs to cassettes and then forward into the digital era—CDs, DVD Audio, Super Audio CD, and online music services, reflect our industry's willingness to embrace new technologies to provide music listeners greater opportunities to access music of ever greater fidelity when and where they want it.

Without question, the Internet challenges us to think about the distribution of recorded music in an entirely different way. Whereas we have been accustomed to the production of physical products embodying creative works, our companies are now fashioning business models applicable to the digital electronic realm. This is a new marketplace in which record companies and their licensees seek to establish a viable, vigorous commercial presence.

Our much publicized skirmishes with Napster, KaZaA, AudioGalaxy, Aimster and various other unauthorized Internet P2P systems enabling the massive uploading and downloading of files of copyrighted music recordings are not prompted by any industry predisposition against the applications or the technology. Rather, it is the very evident fact that the sponsors of those systems are exploiting the creative investment of the performing artists and recording companies for their own commercial benefit, without any intention, or credible effort, to obtain licenses or to pay royalties. It is the misuse of technology that must be stifled, not the technology itself. We believe that P2P technology will offer great benefits for legitimate uses.

Needless to say, these unlawful P2P applications have found almost instantaneous acceptance among college students. This demographic group comprises avid listeners who have traditionally represented a sizeable portion of our retail markets. The scope of illegal P2P file sharing and the consequential detriment to our industry is well known. More than 2.6 billion music files are illegally downloaded every month on unauthorized P2P systems. Of this number, a significant percentage of the transfers occur over campus networks.

This should come as no surprise. After all, American colleges and universities have incredibly fast Internet connections—often as a result of support from the government—which are intended to be used for academic, research and other legitimate purposes. It is to be expected that those who want to engage in file transfers would likely to choose a university system's high bandwidth to do so.

The unauthorized P2P file-sharing problem poses tremendous difficulties not only for copyright owners and artists, but also for administrators on our nations' college campuses. Rampant file-sharing of music and video content imposes a heavy toll on all of us. Despite education campaigns about the illegality of file sharing, and despite numerous court decisions clearly holding that copying music, movies and other copyrighted files is against the law, there is an alarming disregard among students for Internet theft. As a result, P2P abuse has overtaxed numerous college computer systems, slowing processing of legitimate information to a crawl due to the uncommonly large number and size of files being uploaded and downloaded. Moreover, students are often unaware of the dangers of these P2P applications: compromising campus network security, making their own hard drives containing their personal data available to others, and opening the campus network to computer viruses. Even more alarming is the fact that up to 75% of those coming onto the campus networks are people outside the university community who are searching the Internet for the greatest amount of broadband capacity in order to expedite the file transfer. Campus systems, with their fast connections, find themselves hosting total strangers.

Perhaps the newest and most frightening problem emerging on college campuses is what we refer to as LANNs—or Local Area Napster Networks. Apparently, some students have taken it upon themselves to establish Napster-like systems on university campuses, so that students can copy each other's files within the university network, which can often be done more quickly and easily than downloading files from the Internet. Perhaps these students think that what the courts have found to be illegal on the Internet is somehow less illegal if confined to a university network. In fact, such systems are no more lawful, and are primarily being used for the same illicit purposes, as the P2P systems like Napster that have been ruled to infringe our copyrights. We certainly have hope that the university community will actively confront this issue and take steps to stop this development before it spreads.

I'm pleased to say that there have been some very encouraging developments in addressing this problem. The entertainment and higher education communities have undertaken to work together to address the problem of P2P piracy on college campuses. Last fall, RIAA, the Motion Picture Association of America, the Songwriters Guild of America and the National Music Publishers Association jointly sent a letter to 2,300 college and university presidents explaining the severity of online piracy and the importance of their active involvement in tackling the issue. We also reached out to the leadership of the national associations representing the spectrum of the nation's colleges and universities and they demonstrated their support by sending a follow-up letter to the same universities urging them to address the P2P problem proactively. This started a chain of conversations between the content industries and leaders of higher education leading to the establishment of the Joint Committee of the Higher Education and Entertainment Communities. The Co-Chairs of the Joint Committee are Dr. Graham Spanier, the President of Penn State University, who is here today, and my colleague Cary Sherman, RIAA's President. For your reference, I have provided a listing of the principal representatives on each side.

During the initial meeting on December 10, 2002, the Joint Committee decided to establish three task forces focusing on the following areas: Education/Best Practices, Technology, and Legislative Issues.

The Education/Best Practices Task Force, chaired by Dr. John Hennessey, President of Stanford University, is working to identify and develop informational materials that will assist educators and campus administrators in educating students and other members of campus communities about copyrights, their obligation to refrain from infringing conduct, and the institution's commitment to respect the rights of copyright owners. I emphasize that this task force is looking to craft advisory information, recognizing that each institution has its own policies regarding enforcement of computer usage restrictions and disciplinary actions. Some, like the University of North Carolina have exemplary policies. I would like to thank Dr. Molly Broad, who is here today, and I hope that the policy adopted by her university serves as an example to many others. Also, this task force will be sensitive to the concerns of the academic community on matters of privacy, free speech, and academic freedom. We believe that, with active dialogue on these issues, we can make significant headway in lessening the misunderstandings that arise from time to time between the two communities over these issues.

The Technology Task Force, chaired by Dr. Charles Phelps, Provost of the University of Rochester, is taking up an examination of current and emerging technologies that can effectively identify online trafficking of copyrighted material and provide administrators with the resources to limit or prevent infringing uses of P2P systems. The task force will conduct an initial screening of promising technological solutions and then test them in pilot applications on selected campuses. The results will be disseminated to the higher education community affording an opportunity to determine which technologies are of greatest benefit to any given institution. We expect that a number of technologies will show potential. We're not looking for a "one size fits all" outcome.

The Legislative Task Force, co-chaired by Jack Valenti, President of the Motion Picture Association of America, and Dr. Broad, is looking at various issues that have come before Congress that affect both of our communities. This task force will provide an opportunity for both communities to work proactively on emerging issues and to understand the perspectives and concerns of the other. We're confident that this dialogue will strengthen the relationship between us.

To sum this up, we think that we are off to a good start in finding common ground with the leadership representing the nation's colleges and universities. Given that those institutions are themselves heavily invested in copyright and other intellectual property rights, there's every reason to believe that we can forge baseline understandings upon which we can structure effective strategies and programs to educate students and others about music, film, videogame, and software property rights and their legal obligations towards them.

The problems confronting us are formidable. However, we believe that our collaboration with college and universities will bear fruit. Certainly, I would hope that sometime in the near future I will be able to report to you that legitimate on-line music subscription services, which are now becoming abundantly available, have established a viable presence on campuses and that P2P piracy on college networks has receded.

I again thank you for the invitation to speak with you on this topic, and I would be pleased to respond to any questions you may have.

ATTACHMENTS

Entertainment Community Representatives

Roger Ames, Chairman and CEO
Warner Music Group

Matt Gerson, Senior Vice President,
U.S. Public Policy and Government Relations
Vivendi Universal

Sherry Lansing, Chairman
Paramount Pictures

Hilary Rosen, Chairman and CEO
Recording Industry Association of America

Cary Sherman, President
Recording Industry Association of America

Jack Valenti, President and CEO
Motion Picture Association of America

Staff:
Fritz Attaway, Executive Vice President Government Relations
and Washington General Counsel
Motion Picture Association of America (MPAA)

Bruce Block, Senior Vice President for Technology
Recording Industry Association of America

Troy Dow, Vice President and Counsel for Technology and New Media
Motion Picture Association of America (MPAA)

Mitch Glazier, Senior Vice President
Government Relations and Legislative Counsel
Recording Industry Association of America

Barry K. Robinson, Senior Counsel for Corporate Affairs
Recording Industry Association of America

Jonathan Whitehead, Vice President and Anti-Piracy Counsel
Recording Industry Association of America

Higher Education Community Representatives

Dr. Molly Corbett Broad, President
University of North Carolina

Dr. John L. Hennessy, President
Stanford University

Dr. Charles Phelps, Provost
University of Rochester

Ms. Dorothy K. Robinson, Vice President and General Counsel
Yale University

Dr. Graham Spanier, President
The Pennsylvania State University

Staff:
Technology Task Force
Dr. Mark Luker, Vice President
EDUCAUSE

Education Task Force
Mr. Sheldon (Shelley) Steinbach,
Vice President and General Counsel
American Council on Education (ACE)

Legislative Task Froce
Dr. John Vaughn
Executive Vice-President
Association of American Universities (AAU)

Joint Committee of
The Legislative Task Force

Higher Education Representatives

Co-Chair
Molly Corbett Broad, President
University of North Carolina

Rich Jacob, Associate Vice President for Federal Relations
Yale University

Bruce Joseph
Wiley, Rein & Fielding

Pam Lokken, Director, Governmental & Community Relations
Washington University in St. Louis

Matt Peterson, Principal Legislative Analyst
University of California

Bob Samors, Associate Vice President for Federal Relations
University of North Carolina at Chapel Hill

Entertainment Industry Representatives

Co-Chair
Jack Valenti, President and CEO
Motion Picture Association of America

Allan Adler, Vice President for Legal and Governmental Affairs
Association of American Publishers Inc.

Ed Desmond, Vice President, Government Affairs
Interactive Digital Software Association IDSA

Mitch Glazier, Senior Vice President
Government Relations and Legislative Counsel
Recording Industry Association of America

Carl W. Hampe, Partner
Baker & McKenzie

Staff:

Fritz Attaway, Executive Vice President
Government Relations and Washington General Counsel
Motion Picture Association of America (MPAA)

Mike Waring, Executive Director of Federal Relations & Director of the Washington DC Office
University of Michigan

Staff

John Vaughn, Executive Vice President
Association of American Universities

Joint Committee of
The Technology Task Force

Higher Education Representatives

Charles Phelps, Provost, Chair
University of Rochester

Dave Lambert, Vice President & CIO
Georgetown University

Michael McRobbie, VP for Information Technology & CIO
Indiana University

Staff

Mark Luker, VP
EDUCAUSE

Entertainment Community Representatives

Cary Sherman, President
Recording Industry Association of America

Senior Staff:
Bruce Block, Senior V.P.for Technology
Recording Industry Association of America

Other Members:
Dr. Richard Gooch
IFPI

Brad Hunt, Sr. Vice President
Chief Technology Officer
MPAA

Joseph Cates, V.P. Advance Technology
Universal Music Group

Jonathan Whitehead, V.P. Anti-Piracy Counsel
Internet & New Media
Recording Industry Association of America

Mr. SMITH. Thank you, Ms. Rosen.

And Dr. Spanier?

STATEMENT OF GRAHAM SPANIER, PRESIDENT, THE PENNSYLVANIA STATE UNIVERSITY, CO-CHAIR OF THE JOINT COMMITTEE OF HIGHER EDUCATION AND CONTENT COMMUNITIES

Dr. SPANIER. Mr. Chairman and Members of the Subcommittee, I appreciate the opportunity to appear before the Subcommittee today to discuss the important issue of the use of peer-to-peer file-sharing on college and university campuses.

As president of the Pennsylvania State University, I am responsible for the management of an institution that has 24 campuses, 5,000 faculty, and 83,000 students.

The misuse of peer-to-peer technology on college and university campuses is a serious problem that is now acutely confronting higher education administrators. Fully understanding the nature and scope of the problem and how to deal with it raises a series of challenges that we are working hard to meet.

As you've heard, I'm intimately involved in this Committee that is looking at these issues. The purpose of the Committee is twofold: to examine the ways to reduce the misuse of peer-to-peer technology on campuses and to attempt to reduce differences between the higher education and entertainment communities on Federal intellectual property legislative issues.

I believe we have a process that can make real progress in effectively addressing peer-to-peer piracy on university campuses. And I'm hopeful that we can educate our two communities about our common and differing interests and concerns with respect to this and other copyright-related issues.

Higher education is clearly on record in agreeing with the entertainment community that copyright infringement is wrong and that peer-to-peer file-trading that constitutes copyright infringement is illegal and should be stopped. We in higher education understand the concerns of the entertainment industry about the impact of peer-to-peer misuse on their markets and the loss of opportunities that both creators and consumers may suffer as a consequence.

Moreover, university administrators recognize that our institutions have an obligation, through a variety of mechanisms, to educate our students about their legal and ethical responsibilities, not only as members of our university communities, but as members of our society.

We hope, in turn, that the entertainment industry officials and policymakers, such as the Members of this Subcommittee, understand the challenges that lie before university administrators in trying to implement ways to reduce or eliminate inappropriate uses of peer-to-peer without at the same time eliminating legitimate uses of peer-to-peer technologies; without constricting academic freedom and the free and open exchange of information that underpins the creativity, vigor, and productivity of education and research programs; and without invading the privacy of our students, faculty, and staff.

Let me illustrate how these concerns play out at my own university. Penn State has a vigorous program of copyright education for our students and employees. Before getting an account, individuals must agree that they understand and will comply with Federal and State laws in addition to Penn State's acceptable use policies.

We also have an indirect enforcement effort. Audio and video files are large, and we monitor the amount, but not the content, of traffic to and from individual machines. Residence hall users are limited to 1.5 gigabytes of inbound or outbound traffic per week.

There are increasingly severe restrictions for offenders who exceed the limits, beginning with a decrease in the speed allowed for network connection. For persistent violators, there is a complete suspension of network access.

The limitation on bandwidth, coupled with the threat of suspension of access, is intended to discourage copyright infringement. Additionally, when notified by copyright holders of infringement, we comply vigorously with the Digital Millennium Copyright Act and immediately suspend access until the issue is resolved. We received 153 such complaints in calendar year 2001.

Although we do not currently monitor the content to detect the fingerprints of pirated copyrighted material, we would consider such a possibility if technology, functional for a university of our size, allowed us to maintain the educational principles to which we subscribe.

Yet despite these educational efforts, despite our compliance with the Digital Millennium Copyright Act, and despite our technical interventions, it is probably fair to say that thousands of our students illegally download some amount of copyrighted material.

They are typical of college students nationally in this regard and are party to a practice that is morally wrong, is damaging to the entertainment industry, and is inconsistent with the values of honesty and integrity that students more typically profess.

Mr. Chairman and Members of the Committee, I appreciate the interest in this important issue that you all have, and I would be pleased to keep you informed of the work of our joint Committee.

[The prepared statement of Mr. Spanier follows:]

Prepared Statement of Graham B. Spanier

Mr. Chairman and Members of the Subcommittee, I appreciate this opportunity to appear before the subcommittee today to discuss the important issue of the use of peer-to-peer file sharing on college and university campuses. As President of The Pennsylvania State University, I am responsible for the management of an institution that has 24 campuses, 5000 faculty, and 83,000 students.

Penn State has actively and comprehensively incorporated information technology into virtually every aspect of its mission of teaching, research, and service. Computer networks have greatly facilitated communication between students and faculty, have enabled new pedagogical and research capabilities, and have enhanced our campus connections with local communities. Information technology has expanded the educational boundaries of traditional classroom teaching and dramatically increased the potential for distance education.

Beyond academic uses, information technology and networked communications have also improved our ability to establish and maintain personal connections with our alumni, with potential students, and with the public. Email, instant messaging, and personal web sites enable our students' ability to reach each other on campus and connect with the world beyond the campus boundaries with ease.

Unfortunately, the same technologies that so powerfully expand and enrich the academic and personal experiences of our students and faculty can also be misused. The capacity of information technology to be used for both legitimate and illegitimate purposes is clearly demonstrated by peer-to-peer (P2P) file sharing technologies. P2P technology has the potential to expand dramatically the ease, speed, and breadth of information exchange. Such capacity will clearly benefit a wide range of educational and research activities. Indeed, federal agencies such as the National Science Foundation are funding research into P2P development to realize this potential. But P2P can also be used to carry out the unauthorized retrieval and distribution of copyrighted material.

The misuse of P2P technology on college and university campuses—the subject of this hearing—is a serious problem that is now acutely confronting higher education administrators. Fully understanding the nature and scope of the problem and how to deal with it raises a series of challenges that we are working hard to meet.

University officials are working with representatives of the entertainment industry to address the problem of misuse of P2P technology. Last October, two letters—one from entertainment industry organizations and one from the six major national higher education associations—were sent to college and university presidents. The higher education letter urged university officials to examine the use of P2P on their campuses and to take appropriate actions to reduce its misuse.

Last summer and fall, university and higher education association officials also began a series of discussions with representatives of the entertainment industry, culminating in the formation of the Joint Committee of the Higher Education and Entertainment Communities, co-chaired by Cary Sherman, President of the Recording Industry Association of America (RIAA), and me; a list of the full committee is attached to my testimony.

The purpose of the committee is two-fold: (1) to examine ways to reduce the misuse of P2P technology on campuses, and (2) to attempt to reduce differences between the higher education and entertainment communities on federal intellectual property legislative issues. The committee met in December to discuss these issues and how to proceed in addressing them. The committee agreed that we would form three task forces: The first focuses on educational efforts about copyrights, rights and responsibilities, and the appropriate and inappropriate use of P2P file sharing. The second deals with the appropriate role, availability, and functionality of technology in managing P2P use. And the third task force will focus on legislative issues.

The work of the task forces is underway. We expect that they will report back to the full committee later this spring, and we will soon thereafter conclude our formal joint activity with a final review of task force work, formulation of recommendations, and a consideration of final steps.

I believe that we have a process that can make real progress in effectively addressing peer to peer piracy on university campuses, and I am hopeful that we can educate our two communities about our common and differing interests and concerns with respect to this and other copyright-related issues. Higher education is clearly on the record in agreeing with the entertainment community that copyright infringement is wrong, and that P2P file trading that constitutes copyright infringement is illegal and should be stopped. We in higher education understand the concerns of the entertainment industry about the impact of P2P misuse on their markets and the loss of opportunities that both creators and consumers may suffer as a consequence. Moreover, university administrators recognize that our institutions have an obligation, through a variety of mechanisms, to educate our students about their legal and ethical responsibilities, not only as members of our university communities, but as members of our society.

We hope, in turn, that entertainment industry officials and policy makers, such as the members of this subcommittee, understand the challenges that lie before university administrators in trying to implement ways to reduce or eliminate inappropriate uses of P2P without at the same time eliminating legitimate uses of P2P technologies; without constricting academic freedom and the free and open exchange of information that underpins the creativity, vigor, and productivity of our education and research programs; and without invading the privacy of our students, faculty, and staff.

A song downloaded or uploaded by a student using P2P typically constitutes copyright infringement; but in selected cases it might also be a fully legitimate, desired fair use of copyrighted material as part of an educational or research project. A technology may exist or be created that can block P2P transactions, but we would be reluctant to embrace technology that would block both legitimate and illegitimate uses indiscriminately. Nor do we wish to stifle the very creativity and experimentation that has brought us the extraordinary technological capacities that enrich our lives today. Many aspects of this nation's capabilities in information technology and networked communications were developed on research university campuses; we want to be certain that we preserve and nurture that continuing capacity within the academic community for creation and discovery.

Let me illustrate how these concerns play out at my own university. Penn State has a vigorous program of copyright education for our students and employees. Before getting an account, individuals must agree that they understand and will comply with federal and state laws in addition to Penn State's acceptable use policies. The account agreement has a lengthy section dealing with copyright compliance. Likewise, when they get additional services they must agree to policies that include a proscription against copyright infringement.

We also have an indirect enforcement effort. Audio and video files are large, and we monitor the amount, but not the content, of traffic to and from individual machines. Residence Hall users are limited to 1.5 gigabytes of inbound or outbound traffic per week. There are increasingly severe restrictions for offenders who exceed these limitations, beginning with a decrease in the speed allowed for the network connection. For persistent violators there is a complete suspension of network access. The limitation on bandwidth, coupled with the threat of suspension of access, is intended to discourage copyright infringement. Additionally, when notified by copyright holders of infringement, we comply vigorously with the Digital Millennium Copyright Act (DMCA) and immediately suspend access until the issue is resolved. We received 153 such complaints in calendar year 2001. Although we do not currently monitor content to detect the fingerprints of pirated, copyrighted material, we would consider such a possibility if technology, functional for a university of our size, allowed us to maintain the educational principles to which we subscribe.

We also employ proactive technical means to disrupt infringing activities. For example, we routinely scan our networks to find machines that have been compromised in some way or another. One of the primary motivators for intruders to compromise our machines is the establishment of unauthorized outside "Warez" servers, which are generally used for illegally trading copyrighted materials. In just the last few weeks alone, our scanning efforts have located more than 100 such intrusions. Network access to compromised computers is disabled and the illicit software is removed. We also educate the victim whose system has been compromised on how to prevent future compromise of their computer.

Yet despite these educational efforts, despite our compliance with DMCA, and despite our technical interventions, it is probably fair to say that thousands of our students illegally download some amount of copyrighted material. They are typical of college students nationally in this regard and are party to a practice that is morally wrong, is damaging to the entertainment industry, and is inconsistent with the values of honesty and integrity that students more typically profess.

I believe that the work of our joint committee's education and technology task forces will identify a number of useful practices that we intend to share broadly within the higher education community.

One of the great strengths of this country's system of higher education is its extraordinary diversity—public and private institutions, research universities, liberal arts colleges, and community colleges. No single set of policies and procedures for managing P2P technologies is likely appropriate for all, but if we identify a number of educational and technological approaches that have been effective in different settings, we can provide useful examples to colleges and universities that will both encourage and guide them in taking actions appropriate to their local circumstances.

At the same time that higher education officials are developing and implementing educational policies and technological interventions, the content community is developing new business models for marketing copyrighted material, including music and movies. I am hopeful that this combination of effort will go a long way to eliminating the misuse of P2P technologies and facilitate the development of the positive potential of P2P.

The capacity for the illegitimate use of P2P is of course not limited to colleges and universities. Indeed, the entertainment industry has sent letters to private sector companies expressing their concern about such misuse. Moreover, as this nation develops greater broadband capacity throughout society, from K–12 education to home connections, we will face the same potential in many other settings.

This is not a new problem; the nation has faced such challenges with each advance of communications technology—the VCR is but one familiar example. The ideal intellectual property model for higher education today, in this new digital territory, is one that finds appropriate and effective ways of balancing, in the tradition of Copyright law, the proprietary rights of copyright owners and the limitations and exceptions to those rights.

Let me close by saying that I believe higher education is taking seriously its responsibility to deal appropriately with these new intellectual property challenges. I believe our cooperation with the entertainment industry in this effort will help both sectors identify appropriate actions to take. I appreciate the interest of this subcommittee in this important issue, and I would be pleased to keep you informed of the work of our joint committee.

JOINT COMMITTEE OF THE HIGHER EDUCATION AND ENTERTAINMENT COMMUNITIES

Higher Education Representatives

Molly Corbett Broad
President
University of North Carolina

John L. Hennessy
President
Stanford University

Charles Phelps
Provost
University of Rochester

Dorothy K. Robinson
Vice President and General Counsel
Yale University

Graham Spanier (co-chair)
President
The Pennsylvania State University

Staff

Mark Luker
Vice President
EDUCAUSE

Shelley Steinbach
Vice President and General Counsel
American Council on Education

John Vaughn
Executive Vice-President
Association of American Universities

Entertainment Industry Representatives

Roger Ames
Chairman and CEO
Warner Music Group

Matthew T. Gerson
Senior Vice President, U.S. Public Policy and Government Relations
Vivendi Universal

Sherry Lansing
Chairman
Paramount Pictures

Hilary Rosen
Chairman and CEO
Recording Industry Association of America

Cary Sherman (co-chair)
President
Recording Industry Association of America

Jack Valenti
President and CEO
Motion Picture Association of America

Staff

Fritz Attaway
Executive Vice President Government Relations and Washington General Counsel
Motion Picture Association of America

Troy Dow
Vice President and Counsel for Technology and New Media
Motion Picture Association of America

Mitch Glazier
Senior Vice President, Government Relations and Legislative Counsel
Vivendi Universal

Barry Robinson
Senior Counsel for Corporate Affairs
RIAA

Jonathan Whitehead
Vice President and Anti-Piracy Counsel
RIAA

Mr. SMITH. Thank you, Dr. Spanier.

Ms. Render?

STATEMENT OF ROBYN RENDER, VICE PRESIDENT FOR INFORMATION RESOURCES AND CIO, UNIVERSITY OF NORTH CAROLINA

Ms. RENDER. Chairman Smith and other distinguished Members of the Subcommittee, thank you for the invitation to appear before you today to offer one perspective on how representatives from the higher education community are working in collaboration with our counterparts in the entertainment industry to address concerns regarding peer-to-peer file-sharing.

The University of North Carolina is the oldest public university in America, an institution that encompasses 16 diverse campuses, 9,000 faculty, and 177,000 students.

Molly Corbett Broad, president of the University of North Carolina, currently serves on the Joint Committee of Higher Education and Entertainment Communities, which has brought representatives of our respective groups together to examine ways to reduce inappropriate use of peer-to-peer file-sharing technologies on colleges and universities, as well as to explore prospects for narrowing our differences on existing and proposed Federal intellectual property legislation.

President Broad also serves as co-chair, along with Jack Valenti, president and CEO of the Motion Picture Association of America, of this joint Committee's legislative task force. The charge of the task force is to discuss current and proposed legislation on which we differ to see if we can, through candid exploration of the issues, find ways to narrow our differences or develop mutually acceptable alternative proposals.

The relevant issues surrounding P2P are complex, as you are well aware. The Academy brings a unique perspective to these discussions, since intellectual property forms the very essence of the American university. Our institutions have been built, in large part, on the creation of intellectual property and respect for intellectual property of others.

Within the higher education community, such creation and use must be carried out in the context of academic freedom and fair use—interests that are sometimes in conflict with those of the entertainment community.

We are equally committed, however, to addressing unauthorized trading of copyrighted material. Our shared concerns form a common ground that is the basis for serious cooperation and dialogue.

While most universities treat the Internet and attending network services as yet another university forum and resource, it is uniformly recognized that the effective management of these tools must include upholding responsible use of limited resources, protecting the privacy of students, faculty, and staff, and obeying the laws of the land.

Federal legislation that would force policies and practices prohibiting such acceptable and legitimate use of P2P would threaten the central values of the higher education community. We believe a multifaceted approach is needed, a sensible one that emphasizes education and good citizenship; articulates thoughtful, yet adequate policy; utilizes appropriate network management tools; and addresses violations when they occur, but only after due process.

As a representative of the University of North Carolina, let me offer a sampling of how our 16 diverse campuses are addressing these complex issues.

For several years now, our campuses have exhibited leadership in addressing copyright infringement with special emphasis on the issues surrounding student use of P2P applications. During this period, we have monitored increased utilization of bandwidth on UNC campus networks and periodically have carried out our proactive evaluations and policy reviews. All 16 UNC campuses have adopted acceptable use and copyright policies. Our campuses have been working together for the past couple of years to find appropriate ways to manage network traffic resulting from increased P2P traffic.

Traffic from major sites has been monitored and throttled when necessary to protect the campus networks from excesses and unacceptable usage. Several different solutions are applied, however, to the problem, depending upon campus size, network complexity, and culture.

UNC campuses have taken responsibility for educating their students to the legal and moral implications of copyright theft, and we are willing to share our efforts with other institutions.

UNC-Chapel Hill, for example, has created a Web site and a companion document entitled, “Copyright and Acceptable Use on the University Network: A Primer,” which provides answers to frequently asked questions such as: What is fair use? What kind of activities are probable violations of copyright law? What is considered unacceptable use at the University of North Carolina at Chapel Hill? Are MP3s illegal? And what will happen if I get caught?

Looking to the future, the University of North Carolina awaits the results from the Joint Committee of Higher Education and Entertainment Communities Technology Task Force. The staff of this task force will perform an assessment of the various software products that are commercially available for use by higher education institutions to protect resources and prevent infringement.

Once this work is completed, our university will examine past approaches and consider next steps. Fortunately, there are laws that allow the debate regarding how to approach illegal and inappropriate use of P2P to continue with some very appropriate protections intact. We should shape our IT policies around our core academic mission and search for a variety of alternative approaches.

Thank you.

[The prepared statement of Ms. Broad follows:]

Prepared Statement of Molly Corbett Broad

Chairman Smith and other distinguished members of the Subcommittee:

Thank you for the invitation to appear before you today to offer one university president’s perspective on how representatives from the higher education community are working in collaboration with our counterparts in the entertainment industry to address concerns regarding peer-to-peer (“P2P”) file sharing. As president of the University of North Carolina, I am responsible for the management of the oldest public university in America, an institution that encompasses 16 diverse campuses, 9,000 faculty, and 177,000 students.

I currently serve on the Joint Committee of the Higher Education and Entertainment Communities, which has brought representatives of our respective communities together to examine ways to reduce the inappropriate use of peer-to-peer file-sharing technologies on college and university campuses, as well as to explore prospects for narrowing our differences on existing and proposed federal intellectual-property legislation. I also serve as co-chair—along with Jack Valenti, president and CEO of the Motion Picture Association of America—of this Joint Committee's Legislative Task Force. The charge of the task force is to discuss current and proposed legislation on which we differ to see if we can, through candid exploration of the issues, find ways to narrow our differences or develop mutually acceptable alternative proposals. The first meeting of the task force was a casualty of your recent snowstorm, but we are working to reschedule the meeting as soon as feasible.

The relevant issues surrounding P2P are complex, as you are well aware. The Academy brings a unique perspective to these discussions, since intellectual property forms the very essence of the American University. Our institutions have been built in large part on the creation of intellectual property and respect for the intellectual property of others. Within the higher education community, such creation and use must be carried out in the context of academic freedom and fair use—interests that are sometimes in conflict with those of the entertainment community. We are equally committed to addressing unauthorized trading of copyrighted materials. Our shared concerns form a common ground that is the basis for serious cooperation and dialogue.

Most American universities treat the Internet and attending network services as yet another university forum and resource. Technology leaders at these institutions therefore follow the guiding principles of academic freedom and fair use in developing policies and practices for network management and policy administration. While these core values are consistent throughout the Academy, individual institutions vary widely in their academic missions, cultures, and processes for policy development. It is uniformly recognized, however, that effective management of campus resources must include upholding the responsible use of limited resources; protecting the privacy of students, faculty and staff; and obeying the laws of the land. Federal legislation that would force policies and practices prohibiting acceptable and legitimate usage of P2P technologies would threaten the central values of the higher education community.

I believe a multi-faceted approach is needed, a sensible one that emphasizes education and good citizenship, articulates thoughtful yet adequate policy, utilizes appropriate network-management tools, and addresses violations when they occur—but only after due process. As president of the University of North Carolina, let me briefly describe how our 16 diverse campuses are addressing these complicated issues.

For several years now, our campuses have exhibited leadership in addressing copyright infringement, with special emphasis on the issues surrounding student use of P2P applications. During this period, we have monitored the increasing utilization of bandwidth on UNC campus networks and periodically have carried out proactive evaluations and policy reviews. Specific actions taken as a result include:

- In the fall of 2000, the UNC Office of the President conducted a Wide-Area Network Traffic Analysis to assess the need for a University-wide network management strategy.
- All 16 UNC campuses have adopted acceptable use and copyright policies. Our campuses have been working together for the past couple of years to find appropriate ways to manage network traffic resulting from increased P2P traffic. Traffic from major sites for Napster, Morpheus, KaZaa, and others has been monitored and throttled when necessary to protect the campus networks from excessive and unacceptable usage. Several different solutions are applied to the problem, depending upon campus size, network complexity, and culture.
- Using a pass-through state appropriation, UNC contracts for inter-campus networking services with MCNC, a unique corporation that offers access to advanced electronic and information technologies and services for business, government agencies, and North Carolina's education communities. Working with MCNC, UNC campuses are monitoring network traffic consistently and developing appropriate strategies to manage inter- and intra-campus networks effectively as the technologies continuously change and evolve.

- Network management and monitoring tools are available to assist network administrators in managing traffic types and in working within the university policy-setting process to effect policy regarding use of the network. Many UNC campuses are using such tools, and our plans for building out an upgraded inter-campus network include providing such tools to each campus.
- UNC campuses have taken responsibility for educating their students about the legal and moral implications of copyright theft, and we are willing to share our efforts with other institutions. Disciplinary measures should be a part of and consistent with campus student disciplinary procedures. Education and counseling come first, but violations of state and federal law may be prosecuted.

UNC's two research-extensive institutions—the University of North Carolina at Chapel Hill and North Carolina State University—have taken leadership positions on the use of P2P applications by clearly articulating campus policies regarding copyright infringement and the acceptable use of their campus networks. Information sessions with students are held as appropriate to discuss the issue and to provide guidance and notification of sanctions for violations.

UNC-Chapel Hill, for example, has created a web site *(http://www.unc.edu/policy/copyright—primer.html)* and companion document entitled, "Copyright and Acceptable Use on the University Network—A Primer," which provides answers to frequently asked questions, including:

- What is Fair Use?
- What kinds of activities are probable violations of copyright law?
- What is considered unacceptable use at UNC-Chapel Hill?
- Are MP3s illegal?
- What will happen if I get caught?

Looking to the future, the University of North Carolina awaits the results from the Joint Committee of the Higher Education and Entertainment Communities' Technology Task Force. The staff of this task force will perform an assessment of the various software products that are commercially available for use by higher education institutions to protect resources and prevent infringement. Once this work is completed, our University will re-examine past approaches and consider next steps.

As university leaders, we must adapt to changes in technology and the legal landscape in very technical ways, but in doing so, we must remain grounded in the basic, fundamental values of the university and our historic commitment to openness in academic discourse and in the exchange of ideas. Fortunately, there are laws that allow this debate to continue with some very important protections intact. We should shape our IT policies around our core academic mission and values, and we pledge to work with the content community to broaden their understanding of the Academy and our need for varied, alternative approaches.

Thank you.

Mr. SMITH. Thank you, Ms. Render.

Mr. Hale?

STATEMENT OF JOHN HALE, ASSISTANT PROFESSOR OF COMPUTER SCIENCE AND DIRECTOR, CENTER FOR INFORMATION SECURITY, UNIVERSITY OF TULSA

Mr. HALE. Mr. Chairman, Ranking Member Berman, and Members of the Subcommittee, I would like to thank you for the opportunity to come here and speak on an issue that is of extreme importance to our universities and, of course, to copyright owners worldwide.

As an assistant professor of computer science at the University of Tulsa, I've seen media piracy on college campuses pace the evolution and growth of the Internet and now experience a true revolution with peer-to-peer networking.

College students are early adopters of new technology. Unfortunately, many of them have a casual attitude about peer-to-peer file-sharing, and most do not appreciate the security implications of participating in a peer-to-peer network.

Like other universities, we're trying to cope with these problems without sacrificing student liberties. We've responded to complaints of copyright infringement and worked to prevent the continued violations of known infringers. We can also block certain types of peer-to-peer network traffic, while allowing students to use and enjoy a broad spectrum of Internet services.

The Center for Information Security at TU is also doing its part to combat Internet piracy. Changing the mindset of students is perhaps the biggest challenge, but it is our job as educators.

Aside from piracy, another concern is how P2P software clients can produce increased security vulnerabilities. All software has flaws, and some flaws create exposures that can be exploited. Several factors, however, conspire to make security exposures in P2P software much more serious.

First, P2P clients connect systems to massive ad hoc networks that are beyond the administrative control of an enterprise. This dramatically amplifies exposures to external threats. P2P clients are also starting to make use of "tunneling" and "port-hopping" techniques to avoid detection by network firewalls and filters.

Another factor is the emergence of executable media content, such as can be found in Microsoft's Advanced Systems Format and the MPEG–4 standard. The scripting environments that support these technologies can also be abused. E-mail attachments became a popular mode of computer virus transmission only after the introduction of scripting in word-processing documents and Web pages.

The potential impact of self-replicating code on a peer-to-peer network is best seen in the Code Red, Nimda, and Slammer worms that targeted Internet Web servers. In the case of a P2P worm, the damage could be more widespread and much harder to repair. The recipe for this is simple—massive connectivity, exploitable software, and active content. It's probably just a matter of time before a high-profile event occurs.

Yet another factor that affects the integrity of P2P clients is the common industry practice of spyware. The problem here is the trustworthiness of the embedded software. Spyware is also, by construction, difficult to detect and disable.

These threats call for increased technical controls on P2P file-sharing. Techniques for monitoring and filtering traffic have been developed that work and are relatively nonintrusive. Unfortunately, they will become less effective over time as P2P developers integrate encrypted communications.

For this reason, researchers at the Center for Information Security are exploring alternative schemes to protect media in peer-to-peer networks. In particular, we are studying two techniques, interdiction and file-spoofing.

Interdiction swamps the download request queue of a copyright infringer so that other requests are starved out. While this approach need not impair general system or network performance, all download requests to the would-be infringer are impacted, even those that would not constitute a copyright violation.

With file-spoofing, a group of clients flood a peer-to-peer network with search results linked to decoy media. Here, legitimate queries go unaffected, but more research must be done to evaluate how networks respond to large-scale deployment.

Peer-to-peer network technology is elegant, robust, and it has a bright future in computing. But it is experiencing some serious growing pains, and this is nowhere more evident than on our college campuses. It will take a combination of efforts on multiple fronts to help this promising technology survive its adolescence.

Users must be made aware of the risks of installing P2P clients. Attitudes toward piracy must change, and novel anti-piracy technologies should be more closely examined.

In closing, I would like to say that there is a lot at stake, and not just for copyright owners. Thank you.

[The prepared statement of Mr. Hale follows:]

Prepared Statement of John Hale

Mr. Chairman, Ranking Member Berman, and Members of the Subcommittee, I would like to thank you for the opportunity to come before you today and speak on an issue that is of extreme importance to American institutions of higher education and, of course, to copyright owners world-wide.

As an Assistant Professor of Computer Science at the University of Tulsa and as an information security researcher, I have seen media piracy on college campuses pace the evolution and growth of the Internet, and now experience a true revolution with the advent of peer-to-peer (P2P) networking. Broadband Internet access in dormitories and campus apartments has extended the perimeter of the university learning environment to beyond the traditional classroom and laboratory settings. Coupled with P2P technology, it has also created new opportunities for abuse.

In particular, the high bandwidth available to college students and ready supply of music, movies, software and games courtesy of the most popular peer to peer networks have fostered an environment where piracy on a large-scale is not only possible, but commonplace. It is ironic that Internet2 institutions like the University of Tulsa could see a significant fraction of this new bandwidth, which was put in place to foster academic research and collaboration, used for illegal file sharing.

College students are early and aggressive adopters of new technology. Unfortunately, many have an overly casual attitude about file sharing on peer-to-peer networks. Some do not even seem to see any real moral, ethical or even legal dilemma with media piracy over the Internet, and most do not fully appreciate the security implications of exposing a computer to a wide-open P2P network.

Like other universities, The University of Tulsa is trying to cope with these problems without sacrificing student liberties. We have responded to complaints of copyright infringement and worked to prevent the continued violations of known infringers. We also have developed the capability to block certain types of peer-to-peer network traffic, while allowing students to use and enjoy a broad spectrum of Internet services.

Moreover, and most unfortunately, our university may have to soon cap (or throttle) bandwidth in the residential halls at the request of our upstream Internet Service Provider, who provides Internet access to most of the four-year colleges in Oklahoma. This technique reduces the flood of network traffic to an acceptable level, along the way inhibiting (to some extent) mass file sharing, but also impeding any legitimate use of a network that might require substantial bandwidth resources. However, alternative traffic-shaping strategies exist that can pinpoint and mold peer-to-peer network flows with greater precision. The challenge here is in keeping up with new networks and technologies, and in staying on top of the constant game of cat-and-mouse played between P2P developers and enterprise network security architects.

The Center for Information Security within the University of Tulsa is also doing its part to combat Internet piracy and to raise awareness of unsafe computer use practices. Many of our information assurance classes directly address ethics and media piracy, and educate students on security issues and operational risks of running untrusted network applications. Changing the mindset of students is perhaps the biggest challenge, but it is by definition, our job as educators.

Aside from piracy, another major concern is how P2P networking clients installed on university and student-owned computers can result in increased security vulnerabilities in a university network. All software has flaws, and some flaws create exposures that can be exploited to violate the security of a system. Several factors conspire to make the risks induced by security exposures in P2P software much more serious.

The first factor is that P2P clients connect systems to massive ad hoc networks that are beyond the administrative control of any one enterprise. This extreme level of connectivity radically expands the security perimeter of a network. As a result, security vulnerabilities in P2P clients are accessible to every user on that P2P network, regardless of their location. In short, P2P clients dramatically amplify exposures to external threats.

In an effort to maintain a larger network population, P2P client developers have implemented deceptive strategies in their clients to conceal file sharing activity from users and system administrators. Most of the more popular P2P clients do not totally shut down on an exit command from a user. Rather, they fade into the background, continuing to export shared folder contents. It is only when and if a user notices the small client icon in the system task bar that they have an opportunity to leave the file trading network. The goal is obvious: Less sophisticated users will exit the main interface, but not notice they are still connected to the trading network. Another risk confronts less sophisticated users. Haphazard configuration of a P2P client could result in sharing a folder containing sensitive data (instead of music), perhaps even unintentionally sharing the contents of an entire hard drive.

P2P clients are also beginning to make more frequent use of “tunneling” and “port hopping” techniques to avoid detection by network firewalls and filters. Tunneling embeds P2P messages within another protocol so that they blend in with other traffic, and become more difficult for firewalls and filters to detect. An alternative strategy is for clients to vary the communication ports they use (port hop), once again making it more challenging for blocking software to recognize P2P traffic.

Another factor is the emergence of executable media content. Executable media content, such as is found in Microsoft’s Advanced Systems Format and is now possible under the MPEG–4 standard, enriches an entertainment experience by providing multimedia enhancements and greater interactivity. Of course, the expressive scripting and programming environments that support these technologies can also be abused. Email attachments became a popular mode of computer virus transmission only after the introduction of scripting content in word processing documents and web pages.

The weak “viruses” that have been reported on some peer-to-peer networks barely hint at the real potential of self-replicating code in these environments. More suitable examples can be found in the Code Red, Nimda and Slammer worms that targeted Internet web servers. In the case of a true P2P worm, the damage could be even more widespread, it could penetrate deeper into enterprise networks, and due to the stealthy nature of the client software, detection and remediation would be more problematic. The recipe is simple: massive connectivity, exploitable software, and active content. It is probably only a matter of time before a high profile event occurs.

Yet another factor that affects the integrity of P2P clients, is the common industry practice of embedding spyware in them. P2P developers bundle spyware in their clients as a way to generate revenue. Spyware monitors user behavior and tracks user web browsing habits. The information collected by spyware is typically sold to direct-marketing companies. The problem here is the trustworthiness of the embedded software as it is routinely created by unknown third parties. Spyware is, by construction, difficult to detect and may be impossible to disable or remove from a client.

These threats call for increased technical controls on file trading activity in enterprise networks. Techniques for monitoring and filtering P2P traffic have been developed and do work. And some of these strategies may require no more intrusiveness than extracting the “to” and “from” addresses found in packet headers. Even the more sophisticated P2P signature detection schemes do not necessarily reveal who shares what on a network.

Unfortunately, filtering and blocking will become less effective over time as P2P developers integrate additional counter measures. Ultimately, end-to-end encryption of communication channels will make it virtually impossible for system administrators and Internet Service Providers to monitor network traffic. For this reason, researchers in the Center for Information Security at the University of Tulsa are developing and analyzing alternative strategies for protecting digital content in peer-to-peer networks. “P2P Fear and Loathing: Operational Hazards of File Trading Networks,” a white paper we prepared for this Subcommittee in a September 2002 hearing, presents some of our early investigations and is submitted as part of this written testimony. In particular, we are studying two techniques, interdiction and file spoofing, that have been put into practice by some digital rights management companies. These techniques seek to impede copyright infringement through direct participation in peer-to-peer networks.

Interdiction is a technique that swamps the download request queue of a copyright infringer so that other requests are starved out. This counter measure constitutes a high-level Denial of Service attack on a P2P client, but does not necessarily impair general system performance or the performance of the underlying network. One undesirable side effect of this approach is that all download requests to the would-be infringer are impacted, even those that would not constitute a copyright violation.

Like interdiction, file spoofing inhibits copyright infringement through direct participation in peer-to-peer networks. However, while interdiction attacks the download process, file spoofing targets the search process. In this approach, a collection of clients flood a peer-to-peer network with bogus search results linked to decoy media. File spoofing has one advantage in that legitimate queries can go unaffected, but more research needs to be done to evaluate how a network would respond to large scale deployment.

Peer-to-peer network technology is elegant, robust and has a bright future in computing. But it is experiencing some serious growing pains, and this is nowhere more evident than on our college campuses. It will take a combination of efforts on multiple fronts to help this promising technology survive its adolescence. Users must be made aware of the risks of installing and running P2P clients on personal and enterprise networks. Attitudes towards piracy must change. And the potential of novel anti-piracy technologies should be more closely examined. There is a lot at stake, and not just for copyright owners.

ATTACHMENT

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.

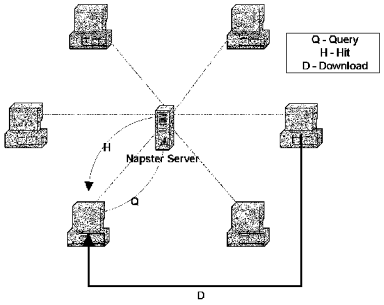


Figure 1: Centralized P2P Model.

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.

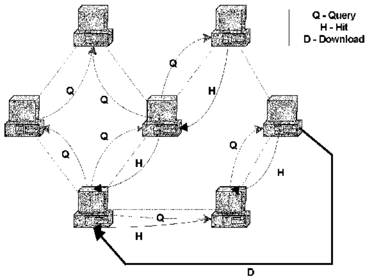


Figure 2: Decentralized P2P Model.

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.

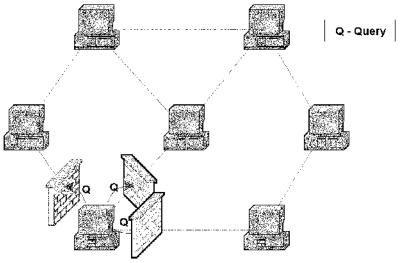


Figure 3: Blocking.

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.

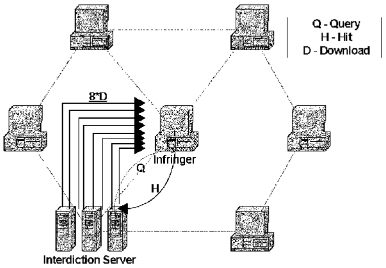


Figure 4: Interdiction.

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.

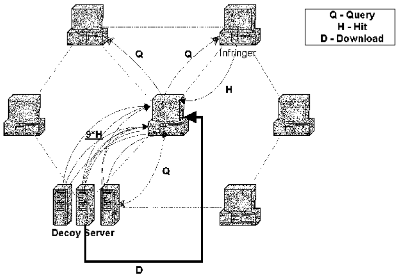


Figure 5: Spoofing.

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.

.

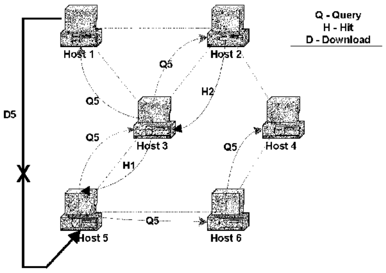


Figure 6: Redirection.

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://www9.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.

Mr. SMITH. Thank you, Mr. Hale.

It seems to me that one of our goals today is to try to determine what model works and also try to measure just how successful the models to date have been. Penn State and UNC have been setting the pace, I think, on college campuses today as to what should be done and can be done. And that sort of will be the line of questioning that I'm going to embark on.

Ms. Rosen, let me direct my first question to you. In your prepared statement—and by the way, I should say to you, I know you've announced that you're going to be leaving your position at the end of the year. We're all going to miss you.

Ms. ROSEN. Thank you, Mr. Chairman.

Mr. SMITH. But I appreciate your being here today, particularly since I know you haven't been feeling well. So thanks for making the effort.

In your prepared testimony, you said you expected a number of technologies will show potential, and you say that you hope in the future that legitimate online music subscription services will have a greater presence on campuses.

But what is the goal of the RIAA? How much do you want to reduce campus piracy? What will you consider to be a success from implementing the education, the enforcement, the technology?

Ms. ROSEN. That's an excellent question and one which doesn't have an easy answer. I think no one is under the illusion that we're going to stop peer-to-peer activity or eliminate online piracy. I think what we want to do, though, is get it to a point where the legitimate business is actually thriving online and so that there is a chance for new investment, new artists, and new opportunities in the online area.

And right now, that's just being drowned out. So that there has been, you know, hundreds of millions of dollars of investment in bringing legitimate services online. And so, we have to find—right now, the balance is somewhere like this. I think we'd like it to be somewhere around here.

Mr. SMITH. Okay. So far, have you seen any appreciable reduction as a result of these various measures?

Ms. ROSEN. No. I think to date what we've seen is that these companies are having an extremely difficult time competing with free, if you will. And in large measure, I think that will continue.

Mr. SMITH. That's a tough business model to compete with, when the competition is free. You're right.

Dr. Spanier, let me go to you, and thank you for your forceful comments as well and for what you're doing on campus.

As a result of these efforts—and as I say, I think you're leading the way—have you seen any reduction because of your educational and enforcement efforts? Have you quantified your success?

Mr. SPANIER. It's hard to know for sure because we have so many students and our networks are so large. I suspect what has happened, if I can guess at the trend, is that the infringement—the gross infringement by smaller numbers of students who, if we provided them unlimited bandwidth, would have continued to explode. That has been curtailed because we do have this—we have, through technological means, narrowed the pipe for them. We're just not permitting massive infringement.

But what I think still exists is that we have thousands of our students who do a modest amount of it, and therein lies the problem. If you have thousands of students at a large university like ours who are doing some of it, you multiply that by all of the college students in the country, it is a problem of the magnitude that several of you summarized.

Mr. SMITH. Right. On the Penn State campuses, what would be your guess as to what percentage you have reduced that illegal downloading? It would be 10 percent or more or less?

Mr. SPANIER. It would be hard to say. Again, I think we have reduced substantially the illegal downloading of some infringers who were doing it in a very substantial way. But we still undoubtedly have a lot of students who are doing some of it.

It's also fair to point out, and I think one could discern this from several of our comments, that for a university like ours, as near as I can tell, somewhere in the neighborhood of three-fourths of the activity on our network——

Mr. SMITH. Is off campus.

Mr. SPANIER. Exactly. Is people coming in from outside and using our students' computers to upload material that is leaving the campus.

We have done something that I don't think very many universities have done. We're employing some proactive technical means to disrupt infringing activities by routinely scanning our networks to find machines that have been compromised in some way or another.

And one of the primary motivators for intruders to compromise our machines is the establishment of unauthorized outside "Warez" servers, which are generally used for illegally trading copyrighted material. Just since January 1st of this year, we have found over 100 such intrusions into computers of our students in our own residence halls.

We go in. We take them off-line. We help them fix their computer, and then we educate them about what's happening. And this really is a very good example of what our technical expert here was describing.

Mr. SMITH. Right. Thank you, Dr. Spanier.

Ms. Render and Dr. Hale, I hope to have a chance to ask you all some questions later on. Right now, I'll recognize the gentleman from California, Mr. Berman, for his questions.

Mr. BERMAN. Well, thank you very much, Mr. Chairman. And I join you in expressing best wishes and appreciation for the work of Hilary Rosen in her stewardship of the RIAA. She is rock-n-roll. No. [Laughter.]

And she gives as good as she gets, and she gets it a lot, and from all sides. And does it with grace and wisdom and skill, and we're going to miss her. But hopefully, this isn't her farewell song today.

The academic witnesses are, in the context of all of this problem, the good guys. They all represent institutions and organizations that are sensitive to the problem, are focused on the problem, are trying to do some things about the problem. And I appreciate that, and I hope you won't take my questions as hostile.

But I do see in your testimony some flaws in your software, and I would just like to exploit them a little bit. That sounds weird. No. [Laughter.]

Let me start with President Spanier. You acknowledge the infringing nature of this activity. But your testimony is reluctant to support blocking P2P transactions because, in selected cases, there might be a fair use?

Mr. SPANIER. Yes.

Mr. BERMAN. In the context of the uploading and downloading we're talking about, where you're spreading it to thousands and thousands of people, could you explain to me that hypothetical case of fair use?

Mr. SPANIER. Yes. Well, as I said only very briefly, there are clearly legitimate uses of peer-to-peer file-sharing. I would agree with Hilary Rosen that that is not typically how that technology is used now.

Mr. BERMAN. I'm just trying—but you talked about there certainly are—there are authorized works being distributed probably that we all know and none of us want to ban P2P networks.

Mr. SPANIER. Yes. Yes.

Mr. BERMAN. So I think we should take that off. That's not something Congress, I think, is seriously contemplating.

But you put it into the context of a fair use, a copyright protected work whose distribution on a P2P system would be a legitimate fair use. And I'm just wondering what that example is.

Mr. SPANIER. Well, the example is not any different than it has been for decades in copyright law in the United States. There are many, many examples when we had printed material, where professors and students and librarians would recognize that it was quite legitimate for instructional, research, and other academic purposes to make fair use of copyrighted materials, which might include using excerpts or taking material and using them in legitimate way in a classroom setting.

And it is also the case that in a digital environment, there may be some legitimate fair use of copyrighted materials.

Mr. BERMAN. Remember, we're talking about distribution on a peer-to-peer system that has millions of people. I'm trying to understand what—I know all kinds of examples of fair use.

Mr. SPANIER. Well, if, for example, we have a faculty member who is in the School of Music or in our program in integrative arts or someone teaching cultural studies who is looking at the impact of certain types of music in our society, and part of a classroom assignment is for students to learn about the music or analyze the lyrics, it would be quite legitimate, I think, to look at that music, to use it, to have it be part of the classroom presentation.

It would be legitimate for a doctoral student who was doing a study of cultural trends to look at these questions. Those would be examples off the top of my head.

Mr. BERMAN. Well, I couldn't agree more. But none of that involves uploading a copyrighted work of music in its entirety onto a system which then allows it to be distributed to millions of people.

Mr. SPANIER. To millions of people? No, absolutely not.

Mr. BERMAN. But that's what this file-trading on P2P systems is.

Mr. SPANIER. Well, quite right, and I would be the first to acknowledge that, that the principal use at the moment of the peer-to-peer file-sharing technology is to illegally download or upload to others copyrighted material. And that is wrong, and that is something we have to cooperatively work at stopping.

What we're concerned about in the higher education community is not throwing the baby out with the bath water. We want to protect fair use in all of its respects, not just in relation to music. This is a much larger issue for our community of librarians and for our network administrators and for our researchers than just music.

Secondly, we want to recognize that there is a lot of marvelous research going on on the use of peer-to-peer networks, which is still in its infancy. And unfortunately, in its infancy, it's mostly being used improperly. But it has great opportunities in the scientific community to be used well, and there are even studies being funded by the National Science Foundation to help work on that technology.

Mr. BERMAN. My time is up, so I don't have any time for more questions. But let me just say in—there are—universities are using blocking technologies to stop legal activities—spam, pornography—because only certain kinds of obscenity which—pornography which meet an obscenity standard are illegal. They're using—and, in many cases, thereby blocking legal transmissions.

They're not drawing some kind of calibration which says because there is something legal that might be taking place, we can't use any blocking technology. There are a thousand different ways to make sure that fair use rights are ensured: e-mails—digitally—e-mails, limited networks that aren't publicly accessible to ensure that this kind of research and collaboration and instruction can take place using copyrighted works in ways that are acknowledged to be fair use.

I just think it's funny to prevent any blocking technology here because there is a theoretical possibility of a fair use, which I can't quite put my finger on, when there are many other ways to distribute it. And then to use that same blocking technology for a variety of other efforts, to stop hate speech and pornography and spam, some of which is clearly legal communications. But thank you.

Mr. SPANIER. There have been efforts to block certain things. It turns out, at this point in time, they're not all that successful because people have found so many ways to defeat them.

But this, in fact, what you've just described, and it's an excellent point, is the charge to our technology Subcommittee, to explore the different technologies that are out there, to study them, sponsor pilot studies, and ultimately to come up with solutions that universities could use if they so choose to use them.

We're not sure a one-solution-fits-all outcome is workable. But we want this Committee to survey what's out there, test it, present them to the university community. And I think when we have that and when we know what's really possible and what will work, I do expect that some universities will adopt some remedies that go beyond what I've described at Penn State.

And as I mentioned in my comments, Penn State would be willing to go even further if we knew that it worked and that it could really be done well, could be ramped up to a university of our size, which, for example, transmits 3 million electronic e-mail messages a day, and not all solutions, it's clear, would work for our systems. We'd be willing to look at something like that.

Mr. SMITH. Dr. Spanier? We need to move on. Thank you for your comments.

Thank you, Mr. Berman.

The gentleman from Tennessee, Mr. Jenkins, is recognized for his questions.

Mr. JENKINS. Thank you, Mr. Chairman.

Dr. Spanier, you perhaps approached this, but nothing has been said about going down to the U.S. Attorneys Office or the local district attorney in an effort to stop this illegal practice.

Has your legal staff, have they gone to the U.S. Attorneys Office or to the district attorney's office in an effort to present whatever cases you may have knowledge of?

Mr. SPANIER. No. We don't typically handle the problem that way. As I mentioned——

Mr. JENKINS. Well, if on your campus, you had an assault and battery or you had a robbery or you had a murder, you would go down to the local district attorney's office, would you not, and consult with them?

Mr. SPANIER. Here's how we view it at the university. We are, first and foremost, educational institutions. The lion's share of our students are in that transition from adolescence to adulthood. So our approach, first of all, is an educational one. We try to educate them.

If that educational approach doesn't work, we restrict their service or deny them access. If we find that they are repeat offenders and trying to circumvent our systems, then they are charged through the university's judicial affairs process, and their status at the university as a student can be affected. They can be suspended, expelled.

We look to those kinds of mechanisms before we would ever want to put this into a criminal situation.

Mr. JENKINS. And you're doing as much as anybody in the country, and I, too, compliment you for it. But let me ask Ms. Rosen, and you're not in this business to provide an educational opportunity, have your folks gone down to the U.S. Attorneys Office or the district attorney's office?

I know there are some statutes. I know early on there were some test cases. They wound up with acquittals. But since then, the law has been changed. And so, have you gone down to the U.S. Attorneys Office or the district attorney's office in the States?

Ms. ROSEN. Well, I think we should separate this into two areas. On the university side, we actually send about 2,500 notices a month to universities around the country when we see egregious users uploading files, making files available. And usually, you know, to a university, they take them down or they deal with the student or they address it.

So, really, where we have—and that's why we're focusing now with the university community on deterrence as opposed to punishment. And what we are looking at, though, in the rest of the world—I mean, there are obviously other bandwidth providers like

ISPs have not been as cooperative as universities are, and that issue, indeed, is in court.

But there are Federal criminal statutes that affect this. And we have also encouraged the Department of Justice to look at deterrence programs because their use is so widespread.

Prosecution on individual basis is extremely difficult. But deterrence might be an avenue for them to go down as well.

Mr. JENKINS. Now, Ms. Render, you were not as sure as the others that those criminal statutes might be effective, as I understood your testimony. Is that right? I believe you said there were considerable roadblocks that were placed in the way of policing this?

Ms. RENDER. I'm not exactly sure which of my comments you are referring to. But let me reiterate that, very similar to Penn State, I mean, we have levels of offense. And what we have found, not being able to quote specific numbers, but on most of our campuses, only about 1 percent are repeat offenders after they have gone through some form of education and an attempt for remediation as to any kind of potential infringement of copyright material.

Talking about some of the, I guess, roadblocks or complications, I think there are still questions about the universities' obligations and responsibilities. I think there are competing laws around privacy and other issues that we have to take into consideration. And so, because it's multifaceted, I think that's the primary reason for a very careful and deliberate approach.

Very encouraged by the potential of the outcome of the work of the technology task force particularly that might give us further information about how we can use the technology in a way that will not be conflicting between those laws of privacy and those laws protecting copyrighted material.

Ms. ROSEN. Mr. Jenkins, could I just comment briefly on the law for 1 minute?

Mr. JENKINS. Sure.

Ms. ROSEN. The law is clear in this area that making files available for the distribution to millions of strangers on P2P networks is illegal. And there has never been an acquittal. The criminal statutes are clear, as the civil statutes are clear. There is no privacy issue associated with that. The——

Ms. RENDER. If I could——

Mr. JENKINS. Well, Ms. Render, if 1 percent of your students at the University of North Carolina were repeat offenders in assault and battery, would you give them the same consideration as you give these offenders, these repeat offenders in this area?

Ms. RENDER. Well, it's my assessment that we treat students pretty consistently regardless of the type of crime or potential crime that is—that they may be accused of. And so, in the very same way, I think that our students are initially given a first chance, an opportunity to be educated and informed. And then as the severity of their conduct or their crime increases, we take more severe action.

Clarifying on my comment, what I was referring to was not a conflict in the law from the standpoint of whether or not copyright is criminal, I was talking about the responsibility a university has as far as following the law of the land and also following laws relative to privacy and protection. As far as things like divulging the names of students, et cetera, was the example I was giving.

Mr. JENKINS. Thank you, ma'am.

Mr. SMITH. Thank you, Mr. Jenkins. The gentlewoman from California, Ms. Waters, is recognized. But Ms. Waters, would you yield to me for a second?

Ms. WATERS. Thank you.

Mr. SMITH. Okay. I wanted to follow up on Mr. Jenkins's question of Ms. Rosen and ask her very, very quickly if you would ever consider taking legal action against individuals?

Ms. ROSEN. Well, right now, nothing's off the table. I think in the university environment, we are extremely optimistic that the universities are not taking the position that Ms. Render just articulated, that they don't have an obligation to notify students of wrongdoing. And even better, that Dr. Spanier and his colleagues are leading a proactive effort on deterrence.

But with regard to the rest of the use, you know, we have clearly and publicly repeatedly said that nothing is off the table now.

Mr. SMITH. Okay. Thank you, Ms. Rosen.

Thank you, Ms. Waters, and you are recognized.

Ms. WATERS. Thank you very much. I'd like to ask any of the witnesses representing universities, have you ever expelled anyone because of the illegal and inappropriate use of a P2P? At Penn State?

Mr. SPANIER. To my knowledge, we haven't expelled anyone. And the reason probably is by the time they get into that zone, if I'm remembering right, we give them three chances at Penn State. By the time they get to that point, we have closed down their access to our networks entirely. They're not allowed to use it, so they don't—they don't get a fourth chance.

Ms. WATERS. But basically, they are allowed to break the law three times before——

Mr. SPANIER. What we do is we're not making a determination at that point about whether they're breaking the law, because we have not gone in and taken their computers to see what's inside of them.

What we have done is given them ample warning that they are exceeding their permitted use of the university's bandwidth, which has given us the suspicion, unless they can come up with a compelling reason, we have assumed that they are illegally downloading——

Ms. WATERS. Doing something illegal. Okay.

Mr. SPANIER [continuing]. Music or videos. And so, when they get to that third infraction, their use is suspended entirely. So that's usually how it ends.

Ms. WATERS. Does anyone else know of any instance where a student has been expelled from university because of the illegal and inappropriate use of P2P?

Ms. RENDER. No.

Ms. WATERS. No? All right. Let me just say this, I'm a little bit torn, a little bit torn about all of this because we encourage our students to be creative and curious and aggressive in the use of new technology, and I think that spirit dominates in this—in this society. And it's too bad that it does come in conflict with—that spirit—with some of the laws relative to copyright.

However, I don't know if I can be of very much help as we discuss this issue because the fact of the matter is the universities of America are not going to criminalize America's middle-class children. You're just not going to do it.

Perhaps if this was taking place in a regional occupation center in an inner-city, where kids were basically stealing other people's intellectual property, we'd see some movement. I don't think this Committee is going to do very much. I don't think the universities are going to do very much.

The fact of the matter is, while I'm sympathetic to the young people, they're breaking the law. And it's a double standard here.

And unless the university is willing to get tough—I mean, this business about "we suspect," and "we have limited the amount of use," and "we go in and we check and we verify," and by that time, it's too late. They have been stealing for 4 years, and then they're gone, I mean, that's just not—that's not acceptable. I mean, you know?

I know what you're saying, and I know what you don't want to do. And I don't think that a public relations campaign—I think it should go on. But I don't think it should be a substitute for hardcore offenders who are in these universities.

And this business about limiting their use, they just go to their friends. I mean, they get together with this, and they go down the hall somewhere and it just continues to go.

And until the university or this Committee is willing to do something about it, we're just wasting everybody's time. I wish I could be more helpful, but it's pretty clear to me.

Thank you, Mr. Chairman.

Mr. SPANIER. If I could just——

Mr. SMITH. Thank you, Ms. Waters.

And, Dr. Spanier, if you'll be very brief in your response?

Mr. SPANIER. Yes, I just want to follow up on what you're saying because I understand your point, and it's an excellent one. But let me point out that the universities are actually trying to do something about this. We do have some opportunities to get a handle on this, and that is what we're working on.

But let me point out that the universities are not the majority of the problem. The majority of what we're describing here is happening outside of the Nation's universities.

Now with bandwidth of the kind we're talking about increasingly available right into the homes and into K–12 and everywhere else, it is a national problem that doesn't just rest squarely on the shoulders of the universities.

So even if we are successful in solving this problem, and we are—we want to. We're working on it. It still doesn't change the fact that it's a broader issue. Hilary and her colleagues sent a letter to corporations across the country asking them to get a handle on this as well.

And so I would just say that as your Committee works on this and takes action, please do keep in mind that the university is one part of the problem. But here we're actually working on it, and the rest of it is still going to be out there.

Ms. WATERS. If the gentleman will yield, today we're just dealing with the university. And of course, wherever crimes are being committed, the law should be applied. And this Committee certainly would support any efforts to use the law against those who are in violation.

But today, we really are just talking about the university today. And just because it is being done outside, it certainly doesn't make it right for it to be done in the corporation or in the university or anyplace else. But I appreciate your problem.

Mr. SPANIER. I agree.

Ms. WATERS. Thank you.

Mr. SPANIER. Thank you.

Mr. SMITH. Thank you, again, Ms. Waters. The gentlewoman from Pennsylvania, Ms. Hart, is recognized for her questions.

Ms. HART. Thank you, Mr. Chairman.

And I happen to agree with Ms. Waters on that point. If it's against the law, it's against the law. And it shouldn't matter whether it's a university student or somebody at home.

I mean, our issue is—I think a large part of it is education, and that is education of young people to the fact that this is wrong, but they need more than that. If there is no consequences, as we all know, there won't be a change in behavior.

Ms. Rosen, I have a question regarding some information we heard from a 2002 Consumer Trends Report that noted that file-sharing is also growing with younger children—teenagers, 12–18, who are not college students. Does the Recording Industry Association have any program where they work with high school students to try to replicate some of the things you're doing on college campuses, first?

And if you are doing that, are you learning—some of the information that you're learning with universities, is that being applied also with the younger children?

Ms. ROSEN. You're right that probably, in some respects, the fastest and most disturbing growth in this area is the 12- to 18-year-old. In some respects, we think that's because it's so penetrated at universities, it's leveled out. There is no more growth. It's just prevalent.

But they're doing it from home, not from their schools. They're doing it because mom or dad has bought broadband access, or they've convinced them to buy it. And so, we have done some—had some conversations at the high school level. And we did a program with Scholastic on this.

But really, it's an education that has to be done more directly with parents. Parents have to feel that they are, in providing the service at their home, doing—putting their kids in legal jeopardy if they're not educating their own kids.

And that's why we've focused our efforts really more at the adults on the legality side and the kids on telling them what the artists and the musicians think about it.

Ms. HART. The universities both, I think, have stated that you do educate the students as to what is proper and correct and legal usage. Have you had any cooperation with schools like, you know, K–12—I guess, not K—but you know, the older kids through senior year at all in cooperation with maybe the high schools in your communities about this? Or is it something that you just do as a responsibility within your own universities?

Ms. RENDER. I think that our focus has definitely been with the incoming freshmen, starting with the incoming freshmen and the students throughout their career at the university. I think, however, though our communications, particularly with the K–12 community and the fact that it's becoming increasingly common for a sharing of education network provisioning between K–12 and the university community, that it's a topic that's being discussed more so with the administrators and technical folk rather than focus on the public relations piece.

Ms. HART. Okay. Thank you. Same at Penn State?

Mr. SPANIER. Yes, we really start the process the day they arrive for freshman orientation, even before they're students. But after they've enrolled in the university, when they apply for their computer account, they have to go through an educational program and agree to certain things before we'll give them an e-mail address and let them onto the network.

Ms. HART. Are they told that there are any consequences for violating——

Mr. SPANIER. Oh, yes. Yes. And by the way, that is—we have a whole program of education that continues. We have posters. We take out advertising. It's fairly extensive. Our efforts to reach the students and to try to get them to understand what's involved here are very extensive.

But you know, it's a little bit like cheating in the classroom. I think any of you who have taught would understand this. When we give—our students basically have been brought up with the right values. They understand—they do understand right from wrong when they come to college. And we have told them, even if they didn't know it already, that it's wrong to be doing what they're doing. And they know it's wrong to cheat in the classroom.

Most of our students want proctors at the exams so there will be no cheating, and there will be an even playing field. And they will then follow the rules. But a lot of students will cheat if they are in a classroom and nobody cares whether they're cheating. And I think we have a little bit of that kind of phenomenon here. It is something that they can get away with, and therefore they do.

And as Hilary and others have said, it's very hard to compete with free. So people are doing it around them, and they have come to convince themselves that it's okay to do this. We're telling them it's not. But I think that's one of the reasons why we're so intent on looking at the possibility of even more significant technical solutions.

Because if we can find a way to prevent it from happening without violating some of the other values that are very important to us in the higher education community, then it's something that many of us would be willing to try, and the students would, of course, just have to accept that.

Ms. HART. Well, I would thank you for that. I know my time is up. But I would really counsel you both, especially from the university community, that as we move forward on this issue, it's only going to get more difficult. And as long as students believe that it's okay to do it, as long as they get away with it, that's the message we're sending, and that's the message the university administration is sending. That's the message that society is sending.

And sure, they may know the difference between right and wrong. But, gee, it doesn't really matter if it's wrong and nobody says anything and nobody does anything about it.

So I would hope that we'll continue to work to find a way to actually eliminate it, prevent the opportunity. But I think, in the meantime, there is nothing wrong with making some examples of some students in the process.

Thank you, Mr. Chairman.

Mr. SMITH. Okay. Thank you, Ms. Hart.

The gentleman from Michigan, Mr. Conyers, the Ranking Member of the full Committee, is recognized for his questions.

Mr. CONYERS. Well, thank you very much, Mr. Chairman. But I'd like to yield to the freshest Member on our side, Mr. Weiner of New York. I mean, the new man on the Subcommittee. [Laughter.]

Mr. WEINER. Thank you, sir.

Can I ask the panel just a little bit about the technological solutions to this technological infringement? And one of the things I'd like to ask you, Dr. Hale, is that the concern that you expressed in your testimony about interdiction as a countermeasure was that it would have the undesirable side effect, in your words, of blocking all download requests, even those that do not constitute a copyright violation.

But that seems to be a small price to pay. I mean, frankly, you're operating in a counterterrorist kind of mode that sometimes you've got to get the person that does it. Is that the only problem, because it seems like interdiction seems like the most promising of the ways to do this?

Mr. HALE. No, that's not the only problem. And I will admit that it is a small problem. I mean, if somebody is pushing drugs and they're also selling popcorn, it makes sense to shut down the entire store until they—until you figure it out.

But there is a legitimate concern over unintended effects of flooding a download request queue. It could cause more serious harm to the system, the entire system that the would-be infringer is running, and maybe also the network——

Mr. WEINER. The would-be infringer, meaning the person requesting the download?

Mr. HALE. No. The person that has the material to be downloaded.

Mr. WEINER. Okay. I'm not persuaded that's a huge problem. But what's next?

Mr. HALE. But also potentially the ISP that that infringer is using. All right? So, you know, maybe there are thousands of people using an ISP, and the infringer is one of them. If you do this poorly, then the potential impact could spread beyond that and affect other people. Now, that's if you do it poorly.

So there may be ways to do it safely, but we don't—there hasn't been a lot of research done on really measuring that, and that's what needs to be done, because it is a promising approach.

Mr. WEINER. Is there, and I'm not sure if it was Ms. Rosen and—is it mister or doctor?

Mr. SPANIER. Either works. [Laughter.]

Mr. WEINER. Well, I don't want to—we're very sensitive about——

Mr. SPANIER. It's doctor. Yes.

Mr. WEINER. Dr. Spanier might have mentioned it.

Is there a way to—are there unique things about music files and movie files that allow you to, from the outside without actually going into the file, kind of scan it as it goes by, pick up identifiers, and say this is a de facto—I mean, close enough. You know what I mean?

Frankly, a 40-page research paper, I imagine, looks differently to a computer scientist than a 2-hour movie.

Mr. HALE. Yes, you can detect the signature of different types of media and determine, you know, without little—with little difficulty, say, well, this is an MP3. Now, you may not—it may take further inspection to conclude it's a copyrighted work, but you can conclude it's an MP3.

And so, that's certainly, you know, within the realm of possibility.

Mr. WEINER. And is that promising? It seems to then deal with the concerns that some of the academics have about not infringing traffic that shouldn't be infringed.

Mr. HALE. It's promising in the short term, but you have to understand the end-game of this entire thing is going to be that it's a big game of cat-and-mouse for the P2P developers. Once this sort of intelligent blocking becomes prominent or prevalent, then they'll begin to encrypt communications. Once they do that, it's——

Mr. WEINER. Yes. But you know, there is a line in the movie "The Untouchables," and I'm sure someone's studio is represented here, where Sean Connery says, you know, "They put one of yours in the hospital. You put one of theirs in the morgue. They come at you with a knife. You come at them with a gun."

I mean, on some level—I think we're on some level pussyfooting around this problem a little bit because of our concern. I mean, there is—you know, we could fill this room with all the file-sharing. Maybe one little corner is what's going on legitimately.

And until we start to kind of do some things to make it clear to the person who's doing the illegal activity that there is some cost, right now, we've really—I mean, not we—you all have, I think, been relatively timid in their approach.

And I don't agree with some of my colleagues that say, you know, lock up a bunch of kids who are downloading Sum 41 songs. But even though if you downloaded—Simon and Garfunkel fans, I think you might get some attention.

But the—I mean, I think that on some level, we in Congress and particularly—I should only speak for myself—want to see some serious action to deal with the problem yourselves before we start tiptoeing up to the line and figuring out what to do.

And if there are concerns that you have about violating the law, then maybe we can come and tweak things to make it possible. But I think, you know, we've been just convening a lot of roundtables and doing a lot of things that I think—you know, I think if some kid had his computer go up in flames because he's downloading a song, the message would get around the Penn State campus pretty quick that that's a bad idea. [Laughter.]

Mr. HALE. I don't know that—I don't know that there's any—I don't know that there's any flame-enabling technology out there. But—— [Laughter.]

Mr. WEINER. No. But there's a guy at Farrell's Bar in Windsor Terrace who will break his kneecaps if he does. I'm not sure we should do that. [Laughter.]

Mr. HALE. Let me respond. I would like to respond by saying I don't think there is anything timid about what, in particular, the Center for Information Security is doing, the approaches we're pursuing.

But you have to understand the thing about encryption is that once those communications are encrypted, we can't tell where they're coming from. It could be somebody buying something off of Amazon.com. We wouldn't know.

So blocking becomes, at the network level, more challenging. So what you have to do is actually participate in the peer-to-peer network to achieve a technological solution, all right? And that's—those are the kinds of things that we're trying to do because we see the end-game is going to be encryption. There's nothing you can do.

Mr. WEINER. And as I yield back, I would say, you know, we here, on the campus here, have firewalls set up. We exchange enormous amounts of information, a lot of research. We even get things right sometimes, and I don't think having those firewalls has brought our work here to a screeching halt. And so——

Mr. BERMAN. Would the gentleman yield?

Mr. WEINER. Well, I'm out of time.

Mr. HALE. If I may respond to that? Firewalls—in the end, firewalls won't work. They just won't work.

Mr. SMITH. Thank you, Mr. Weiner.

The gentleman from California, Mr. Berman, is recognized. You had a follow-up?

Mr. BERMAN. I'll wait.

Mr. SMITH. Okay. The gentleman from Virginia, Mr. Forbes, is recognized for his questions.

Mr. FORBES. Thank you, Mr. Chairman. And I, too, want to echo what everybody said in giving you our appreciation for your being here and to tell you that we honestly do respect your opinions, and that's why you're here.

And I only have 5 minutes. So I'm going to try to be as concise as I can be and ask you three questions. And if you can't answer them now, if you'll just get back with us and give us the answer so we can get them in the record.

The first one is, and I know you don't have specificity on this, but how much do you estimate all of this costs, with as close a parameters as you can get? So we have some feel for just the dollars and cents of what this piracy is costing us.

And the second one, Ms. Rosen, is for you. Are there any universities out there that are doing everything you think they should do? And if so, can you give us a list of those universities and what their model might be?

And then the third question that I have is, up here, we function kind of like a funnel, and it's an interesting funnel because at the top of the funnel we talk an awful lot about the problem. And we'll have hearing after hearing after hearing where everybody comes in and talks about the problem. And you've heard from most of the Members of this Subcommittee they understand there's a problem.

And then you move down to the next level of the funnel, and everybody talks about the parameters. We're concerned about this, but we want to avoid this.

And every great while, we will move down to the bottom of the funnel, where we actually do something. And at that particular point in time, that's what I'm interested in your opinions on. And if you could, and I know you don't have all of the information. We never have all of the information. But I'd like to hear from each one of you, if you could get back to us, what specifically would you like for this Subcommittee to do and, equally important, what would you like for us to avoid doing?

And I commend you, unlike some of my colleagues, for not going out and arresting every kid, you know, that's on campus or making huge examples. I know that's a tough problem. You don't want to put all of them in jail. But we really would like to hear with some specificity what would you like us to do and what would you like for us to avoid doing?

And if you want to respond to any of those in a limited amount of time, that's fine. If not, if you could just get back to us, that would be great.

Ms. ROSEN. Well, as a matter of costs, I think there are multiple costs for the music industry and for the intellectual property industries. I think overall you're talking about, you know, hundreds and hundreds of millions of dollars, jobs, lack of new artists, all sorts of financial consequences that filter down into making less music available for consumers.

Obviously, universities have bandwidth costs and other institutional costs, and I'll leave it to them to try and quantify those.

In terms of what you ought to do, as has been said before, the law is quite good in this area, thanks to a lot of work from a lot of people in this room and on this dais. And so, what we are trying to do is get cooperation on enforcing the law and on deterrence. And where we can't, find creative ways to have the law enforced ourselves in a civil manner.

So, you know, what you have jurisdiction over in terms of resources is Federal jurisdiction, for Federal resources in a criminal area. You have—but in the civil area, I think there's not much more you can do right now to make the law better. It's pretty clear what's being done is illegal.

Mr. FORBES. So you're comfortable with the state of the law, at least, right now? It's just the enforcement part of it?

Ms. ROSEN. I'm comfortable with the state of the law and discomforted about the level of enforcement all around.

Mr. Berman had a creative idea last year, which I was supportive of finding a good way to pursue. And unfortunately, got so caught up in rhetoric and a disinformation campaign that it makes thinking about responsible solutions extremely difficult because of some people's self-interest in avoiding solutions.

So to get more creative, I think, is a big hurdle.

Mr. SPANIER. Universities have costs on both sides of the issue. The additional bandwidth that we have to provide for this illegal activity that's going on and to solve the problems when bad stuff comes in along with music, and our computers are invaded, and we have to go back and fix that.

On the other side, on solving the problem, to deal with all the cases that come to our attention where students are doing something wrong, to go in and remedy those, the enforcement process and these technical solutions require staff time and programming. So we see the costs on both sides.

But I do want to say we're very sympathetic with the very substantial costs that apparently exist on the side of the entertainment industry.

In terms of the end-game, what are we trying to see at the end of that funnel, I just want to take the opportunity to reiterate that we in the university community understand this problem. We are sympathetic with it, and we want to see a stop to it.

This may be perceived as something adversarial. We do not, in any way, see illegally—the illegal pirating of copyrighted material by university students, in any way, to be in the best interests of the university. We would like to put an end to it.

But the bottom line for us is how do we get that done with technical solutions that don't violate some of the most basic principles by which universities have always operated—freedom of speech, freedom of expression, concerns about privacy.

Whether there's a technical solution out there that can deal with this at some gross level without us having to go into a faculty member's or a student's computer, without having to literally scan the content of incoming material that they think they're transmitting privately between colleagues.

If there is a good solution out there that preserves these principles that are so fundamental to higher education, I think we would want to take a very serious look at it, and many universities would adopt it. But there are certain lines we're trying to be very careful not to cross here. We're trying to be very sensitive to that.

Mr. FORBES. My time is up. And thank you all for your help.

Mr. SMITH. Thank you, Mr. Forbes.

We welcome another gentleman from Virginia, Mr. Goodlatte, and he is recognized for his questions.

Mr. GOODLATTE. Thank you, Mr. Chairman. I want to commend you for holding this hearing on a very important issue. It's important to me not only because I have a strong interest in copyright protection, but also because I have more colleges and universities, 22 of them, in my congressional district than any other district in the country. And so, I'm well aware of the nature of this problem.

I do have an opening statement that I'd ask be made a part of the record. And I also want to join in the chorus of congratulations and thanks to Hilary Rosen. As a good Republican, I never thought that I would say about any Democrat named Hilary that "Hilary rocks." [Laughter.]

But that, indeed, is the case here because your work to protect copyright transcends your representation of the Recording Industry Association of America. It is something that is very, very important to the long history we have in this country of building respect for the creation and protection of intellectual property, and it transcends this issue of peer-to-peer networking as well.

So we thank you for your good work, and we know that in your future works, you'll continue to have some involvement with that in some way, I hope.

Let me ask our college representatives something that is of interest to me. Many of the institutions in my district and many around the country have honor codes. And I wonder if any of you have considered whether or not unauthorized file-sharing, which is not only illegal and is certainly a form of theft, whether your institutions consider the theft of intellectual property a violation of your school's moral code of conduct?

And if so, are students informed about the seriousness of unauthorized file-sharing under such a code of conduct?

Ms. RENDER. I'll respond to that, and the answer is yes to that question relative to institutions within the University of North Carolina.

Most of these processes go through the honor system and an honor court from the student standpoint. This type of violation is included in that definition, and they are very seriously revisiting, frankly, various aspects of the honor code, not just for this particular type of infringement, but others that are surfacing on our campuses.

And I'd just like to comment that I think everyone is aware, but emphasize the fact of the iterative nature of this issue. The technology is evolving sometimes faster than we can respond to the processes within our universities. Sometimes they're somewhat painful and deliberate. But there are very good reasons why we have shared governance and inclusion in those processes to ensure that the university community is very well represented.

So I want to emphasize that the serious nature of the issue at hand, I think, is well recognized throughout the university community. We need to, I believe, be given some time for the joint work of the two communities to bear some fruit and some results and given the opportunity as a diverse group of campuses to react to that.

I think scale is another issue that's on both sides. We have very large institutions and very, very small ones. And what it will require will be different for each.

Mr. GOODLATTE. Let me ask you about another aspect of this. One of the more disturbing trends about this has been that students are beginning to develop internal local area networks within universities for file-swapping that does not reach beyond the university's network. And these types of networks do not deplete the university's bandwidth. So that problem that has gotten the attention of some universities is not here and—because they're not using the Internet as a viaduct.

Instead, files are swapped from one computer in the university's network to others within the same network. I believe these local network file-swappings are also illegal, just as illegal as they may be trading over the Internet. And I wonder if any of our university representatives have any thoughts on that issue and whether you've attempted to address that issue in your—in your work?

Mr. HALE. I guess I would like to say that, yes, that's a trend that we've seen, and it's a growing trend and a disturbing one. And it's not necessarily the case that it wouldn't—it would not impact network performance in a university network. It depends upon the architecture of that university's network.

There are—there are things that can be done, and the same types of countermeasures can work. But it's a problem that's a little more difficult to detect and deal with.

Mr. GOODLATTE. Thank you. And Ms. Rosen, if I might ask, in relation to the educational efforts that your industry is undertaking, is there any thought to a massive public relations-type of campaign, coupled—I noted recently that America Online, TimeWarner have just launched a new fee service. A number of other companies have that as well. And that is excellent.

But in order to beat free, there seems to me to be a very strong need for some kind of a general public relations campaign about the effect of peer-to-peer file-swapping on the possible—the principle of file-swapping and the principle of copyright protection.

And I'm just wondering what your industry is doing and what the copyright community at large is doing to have some kind of a massive public relations campaign, to spend tens of millions of dollars in a concentrated effort over a few months' period of time to try to change public attitudes about this?

Ms. ROSEN. You will see tens of millions of dollars spent over the next several months promoting the legitimate services so that consumers will understand that——

Mr. GOODLATTE. But what about the other side of it? That there is——

Ms. ROSEN. On the other side, there has been a public relations campaign which we actually unveiled last fall at this Committee, which received, you know, significant air time on MTV and VH1 and BET, and Clear Channel put it on multiple radio stations around the country.

And we found that that education has had an impact, but there is only so much that education is going to do. There's going to have to be some broader sense, we think, of consequences or significant impact. But I think we'll continue that campaign and, importantly, the legitimate services will go out there.

And I have to say just on the state of the law for 1 second—and this is relevant because it follows up on what Mr. Forbes said. If we lose this pending Verizon case, which I don't think we will—and most of you know about it—I may come back and say the law isn't correct. [Laughter.]

So I have to reserve my option to do that.

Mr. SMITH. Thank you.

Mr. GOODLATTE. Mr. Chairman, I wonder if I might submit one more question for the record?

Mr. SMITH. Sure.

Mr. GOODLATTE. It's directed to Professor Hale, and if he could submit it in writing, he could perhaps respond in writing.

[The prepared statement of Mr. Goodlatte follows:]

PREPARED STATEMENT OF THE HONORABLE BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Mr. Chairman, thank you for holding this important oversight hearing on peer-to-peer piracy on our universities' campuses.

Article I Section 8 of our Constitution lays the framework for our nation's copyright and patent laws. It grants Congress the power to award inventors and creators, for limited amounts of time, exclusive rights to their inventions and works. The founding fathers realized that this type of incentive was crucial to ensure that America would become the world's leader in innovation and creativity. This truth is still applicable today. As we continue our journey into the digital age, we must be sure to continue to reward our innovators with the exclusive rights to their works for limited periods of time. This incentive is still necessary to maintain America's position as the world leader in innovation.

However, the proliferation of copyright piracy in America is growing and is threatening to undermine the very copyright protections our founding fathers envisioned. Particularly disturbing is the growth of piracy on America's university campuses. A recent CNN/USA TODAY/Gallup Poll found that 39% of college students with Internet access admitted to having downloaded music that they did not pay for. A recent study of the FASTTRACK P2P system showed that 16% of the files available at any given moment on the FASTTRACK network were located at IP addresses managed by U.S. educational institutions. Furthermore, 26% of the supernodes on the FASTTRACK network were being run from addresses assigned to universities.

In addition, last year a medium-sized U.S. state university used a prototype network traffic-monitoring tool to provide a snapshot of network usage on its campus. It monitored the activity of 54 users of only one P2P network, the Gnutella network, during the university's summer break. The results of the research showed that 89% of the files transferred to and from the university network were infringing. Furthermore, those 54 monitored users uploaded 4,614 files. In addition, more than 75% of the transferred data was from university users to individuals located outside of the university network, which shows that there is a growing trend toward outside pirates using university resources to download files.

These statistics are nothing short of staggering and show that the problem of piracy on America's university campuses cannot be ignored. Universities should be concerned about copyright piracy for many reasons. I would like to highlight two of these reasons.

First of all, file sharing is theft. When a student downloads a song without paying for the song, that student is stealing. One of the greatest characteristics of our nation's universities is their commitment to honesty and honorable behavior. Most universities demand that students follow strict honor codes that prohibit such activities as lying, cheating and stealing. However, when a university adopts a passive stance on copyright piracy, it sends a mixed message that blurs the moral imperatives it seeks to foster through its honor code.

Secondly, file sharing poses serious security threats to universities' network resources. The simple fact is that P2P networks connect universities' computers to networks that may never have been checked for viruses, worms or other destructive computer codes. This leaves universities wide open to attack. Also, P2P developers often create applications within their software that records users' web browsing behaviors. P2P developers then sell this information to make additional profits. In addition to potential privacy concerns, these tracking applications can be attractive targets for hackers and trespassers looking for weaknesses in universities' networks.

Illegal file swapping is a serious problem for universities. Clearly, industry leaders and university officials must coordinate their efforts to eliminate this illegal activity. I am encouraged by the cooperation exhibited by the parties here today and believe that their efforts to work together to solve these problems are commendable. Through education and the development of best practices and competitive technologies, content providers and educational institutions can show the world that private parties can work together to solve these complex piracy issues without heavy-handed government regulation.

I look forward to hearing from the expert witnesses today regarding the progress the groups are making. I also look forward to receiving the forthcoming reports from the Joint Committee in a timely fashion, and I expect to see documented progress resulting from this cooperation.

Thank you for taking the time to come and talk about your efforts to end copyright piracy on America's university campuses.

Mr. SMITH. Absolutely. And that's a good reminder. Any Member is welcome, if it's all right with the witnesses, to submit questions. Now, before we adjourn, Mr. Berman has a follow-up question.

Mr. CONYERS. Well, Mr. Chairman, would you forget the Ranking Member or what?

Mr. SMITH. Mr. Conyers, you yielded your time to Mr. Weiner. I'll be happy to recognize Mr. Weiner for his time, and he can yield it back to you, if you'd like.

Mr. CONYERS. Oh. So that's the kind of Committee we're going to have—— [Laughter.]

Mr. SMITH. According to the rules.

Mr. CONYERS [continuing]. In the 108th.

Mr. SMITH. In any case, the gentleman from Michigan is recognized if he has some questions.

Mr. CONYERS. Oh, that's very nice of you. Ladies and gentlemen, and Members of the Committee, this is a tough problem. And without a solution, we begin to get into whether people from Farrell's Bar, Mr. Weiner, should be visiting the malefactors or whether the Berman bounty-hunter's notion, which I was sorry to hear Hilary raised, you're going to get some—we're going to take care of this problem in a way you're all going to be very unhappy with.

So I have a solution. Let us all gather around the table and with the electronics industry and with the content industry, let's begin to fashion a solution that we can all live with. Or you'll probably all get a solution that you'll all be very unhappy with.

Can we agree on that? Not yet.

Mr. SPANIER. I think that summarizes quite well why this Committee exists that Cary Sherman and I are co-chairing to try to come up with solutions that we jointly prefer as opposed to something that is imposed on us that may not feel as comfortable.

Mr. CONYERS. Well, Chairman Sensenbrenner, Ranking Member Berman, and the gentleman from Virginia, Mr. Boucher, Mr. Cannon of Utah, a number of us have been meeting on this very same subject. Can we get this behind us in a way that before it gets so big, you're going to get some draconian kinds of results coming out of here?

Now, I don't want to remind anybody about this because somebody may rush to put in a bill. But we did have mandatory minimums on this violation for about 5 years. Mandatory. Criminal. We took it off.

But you know, the general impression that may be happening as a result of this hearing from our distinguished educators is that this is just another visit to Washington, and maybe nothing much is going to happen.

Please, I can assure you that that would—you'd be leaving Judiciary Committee with the wrong impression. Because there are people ready to take action, and it will probably go over the line in terms of privacy concerns and the kind of things that we want.

Now, true, it's a cultural problem. If how many young people say this is a crime, a Federal crime which you could go to the slammer for. And they'd say, please, everybody is doing it, including a lot of their parents, by the way, since we're in the blame thing on kids today. There are a lot of adults doing this same thing. So we have to see from the educational community a ratcheting up of concern about this.

No, you don't have to start throwing kids out of school. The Naval Academy was doing it for a while for these same kinds of infractions that bring us here today. But we do have to make it clear that there is a note of urgent seriousness that has not really manifested itself to the rest of us looking in on what campuses are doing.

So I hope we can all work together and be friends, and I would like anybody that wants to give me any friendly advice on the panel to please do so.

Ms. ROSEN. Keep at it, Mr. Conyers.

Mr. CONYERS. Well, that's easy for you to say. [Laughter.]

We work together so much. But thank you all very much. Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Conyers. The gentleman from California, Mr. Berman.

Mr. BERMAN. Just a couple of observations. One is to sort of reaffirm, as if it were necessary, what Mr. Conyers has said. It is great you're working closely with some of the copyright industries to try and find ways to deal with this problem, but don't let the existence of a process be the answer. The process has to get into concrete steps and deal with the problem, and—and it's important to do it sooner rather than later.

The second observation is to Dr. Hale's comment about encryption. The fact is, yes, encryption can get around the different kinds of blocking efforts. But the encryption also makes the system less usable, less—more difficult for potential downloaders to know what they're downloading. It makes it more complicated.

Things which create—which make things more difficult provide a useful service because they block the frequency and the amount of the infringing activity. And so, in and of itself, the fact that there are countermeasures that can be taken, but which make it more difficult to utilize the peer-to-peer system are not necessarily such a bad consequence.

Thirdly, I just want to make that point on the fair use to Dr. Spanier. You can—if your university class in music wants you to have the fair use advantage of comparing different kinds of music and songs, there are so many different ways of setting up a network for that class, for that school, with respect to these items where you can use a network, but it's not a publicly accessible network that anybody with that software in their computer anywhere in the world can get a hold of.

Because putting it onto that kind of a network that any computer that had the software can get a hold of it is not a fair use. And so, I don't think that notion of the theoretical fair use should block things from happening. There are so many alternatives.

And finally, to Ms. Render, I'd just ask you to revisit the University of North Carolina's network acceptable use policy. Nowhere in that policy, you talk about bandwidth problems and are very specific about certain things you don't want to go on in that network, but you never talk about copyright infringement and that those trades are copyright infringement.

And I'd suggest getting the specificity of that notion into the—into the policy and into the primer that all students who are a part of your network have to get would be useful and specific kind of a statement by the university that that's wrong and should be related directly to infringement.

Mr. SMITH. Thank you, Mr. Berman.

Mr. BERMAN. It's been a good hearing.

Mr. SMITH. Let me make an observation as well, and that is today, as a result of the testimony that we've heard, I've come to kind of a surprising conclusion. And that is that what's been done so far in the way of education and enforcement—and I emphasize so far—really hasn't worked that well.

There hasn't been an appreciable reduction in piracy, and certainly nothing quantifiable that we can point to. And that may well mean that additional steps need to be taken in a number of areas. And so, at least that's one of the conclusions that I've come to as a result of your very, very interesting and worthwhile testimony.

So we thank all of the witnesses for being here today. I thank the Members for their presence as well, and we stand adjourned. Thank you.

[The speech of Mr. Valenti follows:]

PREPARED STATEMENT OF JACK VALENTI

**". . . Man is the only animal
who both laughs and weeps,
because Man is the only animal
who understands the difference
between the way things are
and the way they ought to be"**

Some comments on
the Moral Imperative
offered by

JACK VALENTI, President and CEO
Motion Picture Association of America

at

Duke University
Durham, North Carolina
February 24, 2003

No free, democratic nation can lay claim to greatness unless it has constructed a platform from which springs a moral compact that guides the daily conduct of the society and inspires the society to believe in civic trust. That "moral imperative" connects to every family, to every business, every university, every profession and to government as well. It is defined by what William Faulkner called "the old verities," the words that define what this free and loving land is all about. Words like *duty, service, honor, integrity, pity, pride, compassion, sacrifice.*

If you treat these words casually, if you find them un-cool, if you regard them as mere playthings which only the rabble and the rubes, the unlearned and the unsophisticated, observe and honor, then we will all bear witness to the slow undoing of the great secret of America.

Newspapers have been full of sordid stories of unbounded avarice by some corporate executives, whose acts soiled the moral compact. But their dishonesty did not indict the free market system. The system works. What was so contemptibly wrong was the breakage of civic trust by some within the system who knew they were cheating and stealing from employees and stockholder, but because it was easy to do, because they had the power to do it, they did it.

It was a cynical, coarse defiance of the moral imperative. But the exposure of this fiscal perfidy made most of us think hard and long about the lack of any moral reference within those corporate malefactors.

Most Americans with very little don't resent those who have a lot more. Most Americans believe if they work hard, educate themselves and play by the rules, they will by their own effort rise to higher places and have more tomorrow than they have today. That is the sanity and the beauty of the American dream.

But the belief by the average citizen in the American moral compact is demolished by the brute reality that some who have more got theirs through treachery and trickery, which so cruelly mocked all those "fools" who trusted them.

There is no larger objective in this country than the reassembling of civic trust, the reaffirmation of honorable conduct by the most powerful among us; in short, holding fast to the sustenance of civic trust. How then does the university insert within the young "the old verities" so that students not only understand and believe in the compact but also live it in their daily moral grind? That's the grand question as we enter the new digital world. It's a question that every guardian of the university's purpose must answer.

Someone once said that all movement is not necessarily forward nor is all change necessarily progress. So it is that the digital world is not necessarily a better world, but it is surely a different one. The divide between the digital world and the analog world is a vast chasm. To put it another way, in Mark Twain's words, the difference between digital and analog is the difference "between lightning and the lightning bug." The digital Internet has the potential to become the greatest communications delivery system ever known on this planet. It has the promise of allowing people to find new ways to do new things, and do them with dazzling speed.

The nation's universities, including Duke, are equipped with large pipe, high velocity broadband state-of-the-art computer networks. None better, none faster. They produce vast benefits to the university, allowing instant delivery of information and knowledge for professors and research experts within the academy. They are also accessible to students who are privy to not only this avalanche of data—but also to movies. This is an Open Sesame opportunity for some students to take creative property that does not belong to them with effortless ease and speed. And because they have the power to do it, many, but not all of them, do it.

That is why today I choose to chat with you about the interlacing of the moral compact, digital technology—and American movies—and to introduce you to a view of the collision of values brought on by the migratory magic of digital ones and zeros.

One value says, "Digital technology gives me power to roam the Internet, therefore whatever is available, I can take, no matter who owns it." The other value says, "The fact that digital technology gives me power to use, doesn't make it right for me to use it wrongly." That is where the collision of values takes place.

So it is we confront a contradiction that puts to hazard the moral compact that guides the nation. How does the society deal with it? Importantly, how does the university react to this challenge to civic trust flung down by the best and the brightest?

Viant, a Boston-based research film, estimates that between 400,000 to 600,000 movies are being illegally downloaded EVERY DAY! Sad to report, a large chunk of that Internet abuse occurs on college campuses by students who are hourly visitors to the digital realms of KaaZa, Morpheus, Grockster, Gnutella, etc, so-called "file-swapping" sites and fill their hard drives with new movies, free of charge.

But there is a larger, darker issue here. Students would never enter a Blockbuster store and with furtive glance stuff a DVD inside their jacket and walk out without paying. They know that's shoplifting, they know that's stealing. They know they can find themselves in big-ass trouble if they're caught. That's why they don't do it. Then why would those same young leaders-to-be walk off the Internet with a movie inside their digital jacket? Why? Is it because digital shoplifting is at this moment a "no risk" activity? If that is so, why is it so? Is it because Ambrose Bierce's definition of Conscience as "Something you refer to when you are about to get caught" is an unwanted truth? Are the words "ethics"—"morality"—"principle"—alien words, exiled from the student lexicon? It's a sizeable question.

There are some critics who say, "Come on, movie industry, get with it. Stop your whining and get a new business model."

Fine, except no business model ever struck off by the hand and brain of Man can compete with "Free." And if critics don't understand that, it's because they just love the status quo. When a new multi-million dollar film, just released, is suddenly on the Net being abducted by millions of visitors to file-swapping sites, then that, dear friends, is "the status quo." Not a congenial status. Not a pleasant quo.

About two years ago, when Napster was in full blossom, I spoke to some 200 students, the finest of the breed, at one of the most prestigious universities in the land. My subject was "The Changing American Presidency." In my opening remarks, I said, "Before we talk about the White House, I have a question. Music is not my turf. Movies are. But I wonder how many of you have bought a CD in the last several months?" Some three or four hands were upraised. "Alright, now many of you have been on Napster the last several months?" Every hand shot up.

I fixed my gaze on a young man who I was told was going to graduate near the top of his class. “You are,” I said, “about to graduate from one of the best schools in the world. You are now an educated, civilized human being, those best fitted to meet life’s changes and challenges with versatility and grace. Now, tell me, how do you square that with the fact you’re stealing?”

He was crestfallen at first. Then his face brightened and he said, “Well, maybe it is a kind of stealing, but everyone else is doing it and besides music costs too much.” I smiled as I thought to myself, “for this version of a moral value, parents are paying a small fortune in tuition.”

Making choices is a daily experience for Americans. Making the right choice emerges from a process that is rooted in instinct and intuition which leap from unshakable values. When you come to a fork in the road, which way do you go? If choices chosen by young people early in their learning environment are infected with a moral decay, how then can they ever develop the judgment to take the right fork in the road? How will you, when many of you are in leadership roles in the future, deal with younger employees who have learned as students that if you have the power to take what doesn’t belong to them, you do it? As the leader of the enterprise, how will you come to grips with that? You’ll be face-to-face with the breakage of the moral compact and, guess what; it’s on your dime.

That’s why the university cannot stand aloof from this progression since administrators and professors set the final design before its graduates, in the words of that old cliche—go on to “face life.” I am pleased to report the movie industry is now meeting with a committee representing the nation’s colleges and universities. The objective of these meetings is to urge the construction of a Code of Conduct for students when they use the university broadband system, a Code of Conduct solely within the confines and the authority of the university. Those discussions are going well. The university representatives have a clear vision of this issue. Many of them have developed or in the process of creating a Code of Conduct.

While digital technology is a hyper-modern phenomenon, its molecular connection to the moral rostrum has an ancient ancestry. Many years ago, the British philosopher, William Hazlitt, wrote: “Man is the only animal who both laughs and weeps for he is the only animal who understands the difference between the way things are and the way they ought to be.”

The digital world has the capacity to unlock knowledge hidden behind doors previously only partially open, and mostly closed to all but a few. What is yet to be put in place is a clear understanding of how to conduct yourself when you have digital power available to you that you will not use because it causes injury to others. William Hazlitt summed up that choice for us better than anyone else.

[The Electronic Privacy Information Center letter follows:]

ELECTRONIC PRIVACY INFORMATION CENTER

February 25, 2003

Chairman Lamar Smith
Ranking Member Howard Berman
House Judiciary Subcommittee on
Courts, the Internet, and Intellectual Property
B-351A RHOB
Washington, DC 20515

Re: Oversight Hearing on "Peer-to-Peer Piracy on University Campuses.

Dear Representatives Smith and Berman:

The Electronic Privacy Information Center (EPIC) submits the attached letter for inclusion in the hearing record for the February 26, 2003 Oversight Hearing on Peer-to-Peer Piracy on University Campuses. EPIC sent this letter to college and university presidents, student groups, and other stakeholders in November 2002 to alert them to the risks to privacy and freedom of expression associated with monitoring peer-to-peer network traffic. Further, the EPIC letter recommends approaches to peer-to-peer piracy that do not impinge on individuals' privacy and are consistent with higher education values.

EPIC is a not-for-profit research center based in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. If we can be of further assistance on this matter, please do not hesitate to contact us.

Sincerely,

Marc Rotenberg
Executive Director

Chris Hoofnagle
Deputy Counsel

ELECTRONIC PRIVACY INFORMATION CENTER

November 6, 2002

Dear College or University President,

We are writing in regard to a series of letters you recently received on issues of copyright infringement and peer-to-peer (P2P) file trading networks.[1] The Electronic Privacy Information Center (EPIC) is a not-for-profit research center that focuses on the right to privacy and emerging civil liberties issues. We believe these issues require a circumspect analysis of the impact of network monitoring on privacy and academic freedom. While network monitoring is appropriate for certain purposes such as security and bandwidth management, the surveillance of individuals' Internet communications implicates important rights, and raises questions about the appropriate role of higher education institutions in policing private behavior.

We recommend that your institution carefully consider the issues recently detailed in a report by the National Science Foundation Logging and Monitoring Project (LAMP).[2] The LAMP report examines the intersection of network logging, privacy issues, and security risks. It also recognizes the unique environment of higher education institutions, and recommends caution when engaging in monitoring.

While the Recording Industry Association of America (RIAA) has legitimate interests in protecting against infringement, it is worth noting that copyright law sets limits on the exclusive rights of content owners, making some uses of protected material legal.[3] The copyright trade association approach has not always been sensitive to these different types of uses, while raising significant privacy and speech concerns.[4] Now, the RIAA wishes to involve colleges and universities in the process of policing the communicative activities of students, staff, and faculty in a way that is significantly outside institutional missions. For this reason, and the considerations listed below, we urge caution in

[1] Letter from Hillary Rosen, Chairman and CEO, Recording Industry Association of America, to College and University Presidents (Oct. 3, 2002), at http://www.riaa.com/pdf/Universityletter.pdf; Letter from David Ward, President, American Council on Education, to College and University Presidents (Oct. 9, 2002), at http://www.riaa.com/pdf/Copyrightletter.pdf.

[2] Virginia E. Rezmierski & Nathaniel St. Clair, II, Identifying Where Technology Logging and Monitoring for Increased Security Ends and Violations of Personal Privacy and Student Records Begin, Final Report of the National Science Foundation Logging and Monitoring Project (2001), at http://www.aacrao.org/publications/catalog/NSF-LAMP.pdf.

[3] See 17 U.S.C. §§ 107-122, 1008.

[4] Jessica Litman, War Stories, 20 Cardozo Arts & Entertainment Law Journal 337 (2002) (forthcoming), at http://www.law.wayne.edu/litman/papers/warstories.pdf; John Markoff, Scientists Drop Plan to Present Music-Copying Study That Record Industry Opposed, New York Times, Apr. 27, 2001; Legal Concerns Delay Publication of Research on 'Digital Watermarks,' Chronicle of Higher Education, Feb, 9, 2001.

adopting network monitoring and other similar methods to address concerns about infringement.

Network monitoring can have a chilling effect on the marketplace of ideas. It is critical that higher education institutions set policies that foster open-mindedness and critical inquiry. As Chief Justice Earl Warren noted in *Sweezy v. New Hampshire*, "Teachers and students must always remain free to inquire, to study and to evaluate, to gain new maturity and understanding; otherwise our civilization will stagnate and die."[5]

Monitoring the content of communications is fundamentally incompatible with the mission of educational institutions to foster critical thinking and exploration. Monitoring chills behavior, and can squelch creativity that must thrive in educational settings. Furthermore, in order to monitor at the level desired by the copyright industry—to detect file transfers "without authorization"—institutions would have to delve into the content and intended uses of almost every communication. Such a level of monitoring is not only impracticable; it is incompatible with intellectual freedom.

Monitoring individuals' network usage leads to data protection responsibilities. Monitoring of individuals' network usage habits generates records subject to a system of protections under the Federal Educational Rights and Privacy Act (FERPA).[6] In addition to the protections provided by FERPA, a 1997 report by CAUSE (Association for Managing and Using Information Resources in Higher Education) recommends a full system of Fair Information Practices (FIPs) for the treatment of these student records. This framework includes notification of policies; minimization of collection of data; limits on secondary use; nondisclosure and consent; a need to know before granting third parties access to data; data accuracy, inspection, and review; information security, integrity, and accountability; and education.[7]

Network monitoring appliances can be systems of general surveillance. The RIAA has recommended widespread use of network monitoring to manage P2P file sharing. These technical approaches can become systems of surveillance. Once installed on an institution's network, they could be used for copyright control today, and the control of ideas tomorrow. Institutions should not build in a network infrastructure that facilitates monitoring because "[w]hat may begin as logging activity to protect the efficient and effective functioning of one system can become targeted data collection and surveillance of a specific individual."[8]

Free environments shun technological controls on behavior. Because individuals at institutions of higher education must always remain free to inquire, colleges and universities are not the place for technological restrictions on communication.

[5] 354 U.S. 234 (1957).

[6] 20 U.S.C. § 1232g.

[7] Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities, CAUSE, April 1997, at http://www.educause.edu/ir/library/pdf/pub3102.pdf.

[8] Rezmierski & St. Clair at 1.2. Further, "College and university communities are vulnerable to unwitting as well as purposeful abuses of network and information systems." Id. at 1.1.

Institutions of higher education should not practice content monitoring, an approach that the controlled environments of corporate workplaces and kindergartens have adopted.

Further, institutions that simply install a network monitoring application circumvent deliberative academic policymaking. All stakeholders of the university—including students—must be involved in a process that recognizes the legitimate concerns of the copyright industry without unduly hindering academic freedom, privacy, and fair use rights. As Professor Virginia Rezmierski and Aline Soules have noted:

> For a policy to be effective in guiding community behaviors, it must reflect the full range of the community's values, must be understood and embraced by community members, and must reinforce the most important values and the mission of the institution as a whole. An effective policy requires campus-wide discussion and the involvement of each of the major constituencies of the community.[9]

The purported privacy and security risks of P2P are largely red herrings. The copyright industry alleges that P2P programs jeopardize network security and privacy. While all network-enabled applications raise security concerns, P2P systems are not uniquely vulnerable and do not warrant special treatment on these grounds. Far more damage to data integrity and privacy results from exploits of Microsoft Outlook than from P2P applications. Academic institutions have not responded to Outlook-based security threats with prohibition or surveillance; instead, measures are put in place to limit entry of known threats and educate network users about appropriate protection measures.

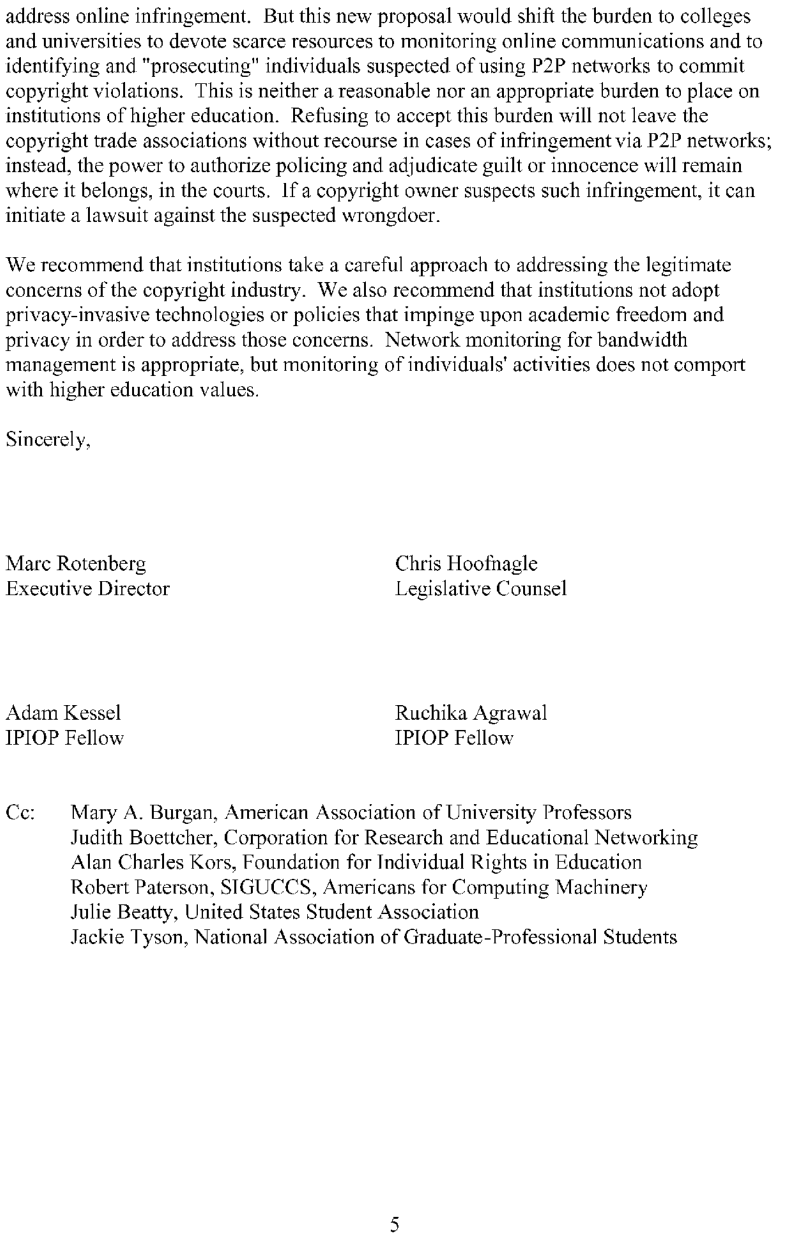
Network surveillance and enforcement is likely to lead to an escalating network "arms race," potentially harming overall network integrity and performance. While P2P traffic currently travels over easily identifiable TCP ports, if these ports are blocked or unreasonably throttled, it is likely that this traffic will move to less easily filtered modes. Certain P2P clients already use port 80 (usually reserved for Web browsing) when they detect the presence of a firewall blocking other ports.[10] Furthermore, file sharing applications utilizing sophisticated encryption already exist,[11] and are likely to become widely deployed in response to efforts to limit these systems. Academic institutions should not adopt a confrontational role with respect to these technologies. By permitting reasonable use of these applications, they can ensure that the traffic remains identifiable for purposes of efficient bandwidth allocation without the use of needlessly privacy-invasive techniques.

Under current law, educational institutions are required to take down infringing content hosted on a university Web server. These provisions provide an adequate remedy to

[9] Virginia E. Rezmierski & Aline Soules, Security vs. Anonymity: The Debate over User Authentication and Information Access, EDUCAUSE Review (March/April 2000), at http://www.educause.edu/ir/library/pdf/ERM0022.pdf

[10] http://www.groove.net/.

[11] http://www.freenetproject.org/.



address online infringement. But this new proposal would shift the burden to colleges and universities to devote scarce resources to monitoring online communications and to identifying and "prosecuting" individuals suspected of using P2P networks to commit copyright violations. This is neither a reasonable nor an appropriate burden to place on institutions of higher education. Refusing to accept this burden will not leave the copyright trade associations without recourse in cases of infringement via P2P networks; instead, the power to authorize policing and adjudicate guilt or innocence will remain where it belongs, in the courts. If a copyright owner suspects such infringement, it can initiate a lawsuit against the suspected wrongdoer.

We recommend that institutions take a careful approach to addressing the legitimate concerns of the copyright industry. We also recommend that institutions not adopt privacy-invasive technologies or policies that impinge upon academic freedom and privacy in order to address those concerns. Network monitoring for bandwidth management is appropriate, but monitoring of individuals' activities does not comport with higher education values.

Sincerely,

Marc Rotenberg Executive Director	Chris Hoofnagle Legislative Counsel
Adam Kessel IPIOP Fellow	Ruchika Agrawal IPIOP Fellow

Cc: Mary A. Burgan, American Association of University Professors
Judith Boettcher, Corporation for Research and Educational Networking
Alan Charles Kors, Foundation for Individual Rights in Education
Robert Paterson, SIGUCCS, Americans for Computing Machinery
Julie Beatty, United States Student Association
Jackie Tyson, National Association of Graduate-Professional Students

[Whereupon, at 12 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress From the State of Michigan

One middle-ground approach to stopping piracy seems to be working: for the industries to negotiate privately and then for the government to mandate the agreement so that it can be enforced. This already has happened with the broadcast flag issue, which revolved around how to make sure that DVD players and computers would recognize and obey the rights management on broadcast digital TV signals. The parties agreed on how to approach this and the FCC is working on a rule to mandate the agreement.

These negotiations must continue and resolve these peer-to-peer issues. Copyright piracy is one of the most serious economic problems facing this Committee. As the whole world knows by now, we have absolutely rampant piracy over the Internet. Consumers have grown accustomed to free music on the Web; movies and video games are not far behind.

In the meantime, I believe that one potential solution is for an institution not to monitor student activity on the Internet, but to warn students when a third-party, typically the recording industry, notifies the university of an alleged transgression. The student is then asked to remove the offending conduct and to stop the file-sharing.

I think that it is critical that higher education institutions set forth policies that foster open-mindedness and critical inquiry. I also believe that network monitoring has the potential to stifle the creativity and academic freedom among students that must thrive in educational settings.

There is no doubt in my mind we are at a crossroads in the content business. The decisions we make this year in Congress, the state legislatures, and the courts will have an impact on the future of the content industry, and whether we will even have a viable content industry in the future.

So it is altogether fitting that we begin the Subcommittee's agenda with a hearing concerning peer-to-peer networks in college communities. File sharing among students can provide many beneficial uses in education, research, and professional development. Unfortunately, many students on university campuses have exploited the intended use of the peer-to-peer network, engaging in the practice of trafficking music, movies, software, video games, and other copyrighted material without permission. Aside from raising issues of copyright infringement, this illegal use of the peer-to-peer network can lead to invasions of student privacy, viruses, and other potential security threats to the university's network.

Last year, consumers swapped over 5 billion music files over peer-to-peer networks. An astonishing 58 percent of the American population between the ages of 12–21 have downloaded MP3s over the Internet in the past two years. That amounts to hundreds of billions of dollars that are being stolen from creators. Clearly this degradation and exploitation of what should be a beneficial system will continue to have a deteriorating effect on our economy, not to mention our livelihoods as consumers in the content industry, if it is allowed to continue.

The content industry is stepping up its battle against digital copyright piracy on college campuses, encouraging higher education leaders to monitor their students and impose restrictions on violators. Those who oppose network monitoring argue that, aside from raising privacy concerns, such monitoring can have a chilling effect on the use of the peer-to-peer technology that can otherwise have valuable academic rewards. The end result, they claim, would amount to an overall chilling effect on the marketplace of ideas.

Monitoring can have the effect of turning university officials into spies for the content industry, thus creating an atmosphere in which the First Amendment and privacy rights of students are significantly devalued. Piracy, however, has proven to be a lethal threat to the content and technology industries and universities must take care to address these legitimate concerns that continue to plague the copyright industry.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

The Honorable Lamar S. Smith
Chairman
Subcommittee on Courts, the Internet,
  and Intellectual Property
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

On behalf of the Department of Justice, we commend you for your dedication to addressing the growing threat of copyright piracy and for holding a hearing on the issue of peer-to-peer use at universities. With significant Congressional support, the Department has taken major strides in the past few years to combat copyright piracy in all of its forms, and we look forward to working with you on this and other issues in the future. The Department is pleased to share with you and the Committee some thoughts on the issue of peer-to-peer systems and universities.

It is important at the outset to acknowledge the Department's firm belief in the virtues of the Internet. In too many instances, people view government officials, especially those who work in federal law enforcement, as anti-technology – intent only on stifling the growth of technology and the Internet. This is simply not the case. The Internet's benefits are too numerous and obvious to restate here and we support the full development of the Internet and technology. But, just as law enforcement must operate in a way that does not unnecessarily impede the advancement of technology, so too must our critics acknowledge the need to address criminal conduct, whether it occurs in physical space or online.

Based upon investigations that we have conducted across the United States, and in dealing with various defendants in these cases, there can be little doubt that individuals exploit university computer networks both here and abroad to engage in a wide array of infringing activities. While peer-to-peer networks operated on university networks are a significant source of infringing and potentially criminal activity, university systems are also being used for other infringing conduct. For example, investigation has revealed that in addition to peer-to-peer, individuals have used university systems:

- to run Internet Relay Chat (IRC), used by pirates to communicate, or solicit new members into the piracy community;

- to operate File Transfer Protocol (FTP) servers, which can allow others to download pirated products;
- and to host major computer sites, containing literally hundreds of thousands of copies of pirated music, movies, software and games, especially by some of the most prominent international piracy, or "warez" groups.

University systems, due to their size and volume of users (which makes it easier to avoid detection) and their large bandwidth capacity (which makes downloading of large files easier and faster), are prime targets of the illegal warez trade. In fact, we have learned that on many of the publicly accessible IRC channels, it is not uncommon to find individuals soliciting people with ".edu" usernames to host small warez sites on their computers on university systems. People recruited in this fashion are asked to host a small cache of pirated music, movies, games or software, which is generally made available to the public for unauthorized reproduction. By distributing pirated products across a wider range of computers in this manner, groups hope to avoid attention, as well as the significant losses that would be suffered if one single, very large site were removed as a result of industry or law enforcement action.

In addition to facilitating illegal activity, the drain on university resources by this type of conduct is substantial. In one recent investigation, the Department executed a series of warrants at seven universities simultaneously, seizing computers operated by system administrators and students alike. All were engaged in large-scale software piracy. At one of the universities where warrants were executed, we were informed that, shortly after the seizures, the university witnessed a 65% decrease in bandwidth usage. This enormous drop in usage simply could not have occurred as a result of removing the handful of computers from the network, rather, it was attributable to the news circulating that law enforcement was on the system investigating illegal activity. Clearly, university systems are one of many mediums being exploited by individuals and groups engaging in infringement, be it civil or criminal in nature. The hearing you are holding today will no doubt shed much needed light on this situation and provide the American people with a deeper understanding of the threat of piracy in the digital age.

In closing, the Department looks forward to working with you and the Congress on this and other piracy-related issues in the months ahead. With the support of Congress we have had many successes in the recent past, and look forward to greater achievements in the future. While emerging technologies, such as peer-to-peer, pose new challenges to rights holders, the Department is and will remain committed to strong enforcement of our criminal intellectual property laws.

The Honorable Lamar Smith
Page 3

If we can be of further assistance on this or any other matter, please do not hesitate to contact this office.

Sincerely,

Jamie E. Brown
Acting Assistant Attorney General

cc: The Honorable Howard Berman
Ranking Minority Member