THE ROLE OF TECHNOLOGY IN REDUCING ILLEGAL FILESHARING: A UNIVERSITY PERSPECTIVE

HEARING

BEFORE THE

COMMITTEE ON SCIENCE AND TECHNOLOGY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 5, 2007

Serial No. 110–34

Printed for the use of the Committee on Science and Technology

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

U.S. GOVERNMENT PRINTING OFFICE
35–706PS WASHINGTON : 2007

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE AND TECHNOLOGY

HON. BART GORDON, Tennessee, *Chairman*

JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
MARK UDALL, Colorado
DAVID WU, Oregon
BRIAN BAIRD, Washington
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
NICK LAMPSON, Texas
GABRIELLE GIFFORDS, Arizona
JERRY MCNERNEY, California
PAUL KANJORSKI, Pennsylvania
DARLENE HOOLEY, Oregon
STEVEN R. ROTHMAN, New Jersey
MICHAEL M. HONDA, California
JIM MATHESON, Utah
MIKE ROSS, Arkansas
BEN CHANDLER, Kentucky
RUSS CARNAHAN, Missouri
CHARLIE MELANCON, Louisiana
BARON P. HILL, Indiana
HARRY E. MITCHELL, Arizona
CHARLES A. WILSON, Ohio

RALPH M. HALL, Texas
F. JAMES SENSENBRENNER JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
KEN CALVERT, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
JO BONNER, Alabama
TOM FEENEY, Florida
RANDY NEUGEBAUER, Texas
BOB INGLIS, South Carolina
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
MARIO DIAZ-BALART, Florida
PHIL GINGREY, Georgia
BRIAN P. BILBRAY, California
ADRIAN SMITH, Nebraska
VACANCY

CONTENTS

June 5, 2007

THE ROLE OF TECHNOLOGY IN REDUCING ILLEGAL FILESHARING: A UNIVERSITY PERSPECTIVE

TUESDAY, JUNE 5, 2007

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, DC.

The Committee met, pursuant to call, at 2:05 p.m., in Room 2318 of the Rayburn House Office Building, Hon. Bart Gordon [Chairman of the Committee] presiding.

BART GORDON, TENNESSEE
CHAIRMAN

RALPH M. HALL, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON SCIENCE AND TECHNOLOGY

SUITE 2320 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6375
TTY: (202) 226–4410
http://science.house.gov

Hearing on

"The Role of Technology in Reducing Illegal Filesharing:
A University Perspective"

2318 Rayburn House Office Building
Washington, D.C.

Tuesday, June 5, 2007
2:00 p.m.

WITNESS LIST

Dr. Charles Wight
Associate Vice President for Academic Affairs and Undergraduate Studies
University of Utah

Dr. Adrian Sannier
Vice President and University Technology Officer
Arizona State University

Mr. Vance Ikezoye
President and CEO
Audible Magic Corporation

Ms. Cheryl Asper Elzy
Dean of University Libraries
Illinois State University

Dr. Greg Jackson
Vice President and Chief Information Officer
University of Chicago

HEARING CHARTER

COMMITTEE ON SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

The Role of Technology in Reducing Illegal Filesharing: A University Perspective

TUESDAY, JUNE 5, 2007
2:00 P.M.–4:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

On Tuesday, June 5, 2007, the Committee on Science and Technology of the U.S. House of Representatives will hold a hearing to learn about the experiences of universities that have implemented technological measures to reduce copyright-infringing filesharing on their campus networks. University representatives and a leading technologist will discuss the nature of these technologies, their potentials and limitations, techniques for evaluating and testing them in realistic settings, and their experiences using them.

2. Witnesses

Dr. Charles Wight is the Associate Vice President for Academic Affairs and Undergraduate Studies at the University of Utah.

Dr. Adrian Sannier is the Vice President and University Technology Officer at Arizona State University, on leave from Iowa State University.

Mr. Vance Ikezoye is the President and CEO of Audible Magic Corporation of Los Gatos, California.

Ms. Cheryl Asper Elzy is the Dean of University Libraries at Illinois State University and a member of the management team of ISU's Digital Citizen Project.

Dr. Greg Jackson is the Vice President and Chief Information Officer at the University of Chicago.

3. Brief Overview

- Most colleges and universities provide high-speed Internet access to their students, faculty and staff. These campus networks are intended for education and research, but they are often used for entertainment or other purposes as well. Over the past several years, free peer-to-peer (P2P) filesharing programs have made it easy for college and university students to illegally download and share copyrighted music, movies, and other content via their campus network connections. In 2005, copyright-infringing filesharing in the U.S. cost the movie industry $500 million, an estimated 44 percent of which was due to college and university students. In 2006, some 1.3 billion music tracks were downloaded illegally in the U.S. by college students, compared with approximately 500 million legal downloads.
- Under the "safe harbor" provision of the *Digital Millennium Copyright Act* (DMCA) of 1998, colleges and universities are not held liable for copyright-infringing filesharing conducted on their campus networks, provided that they cooperate with copyright holders to identify and deal with users on their networks who illegally share copyrighted materials.
- Many college and university campuses have adopted technological measures to prevent illegal filesharing on their networks. These measures fall into two general categories: "traffic-shaping" systems, which control the speed of network transmissions based on where in the network they originate and what computer program sends them; and "network-filtering" systems, which specifically identify and block transmissions that contain copyrighted material. The use of traffic-shaping technology is relatively common, and a majority of cam-

puses now employ it to improve the performance of their campus networks. Network-filtering technologies have not yet been as widely adopted.

4. Issues and Concerns

What has been the overall experience of campuses that have implemented technological measures to reduce illegal filesharing? A significant majority of U.S. campuses are using traffic-shaping systems to control and modify the rate of file transmission on their networks. Campuses "shape" the traffic on their networks by modifying the rate at which different types of files are transmitted, based on which part of campus the data is coming from, what type of program is transmitting the data, and other factors. Most campuses have had a positive experience with this type of technology and do not report any significant complaints or concerns about its use. A smaller number of campuses have deployed network-filtering systems that specifically identify and block copyrighted materials in transmitted files. The experience of these universities with these technologies will be valuable input for other campuses that are considering which technological measures are appropriate to take in reducing illegal filesharing, and also in discovering what technical issues may arise in the deployment of these technologies on campus networks.

Have technological measures been successful in reducing illegal filesharing on campuses? Campuses that have adopted technical means to reduce illegal filesharing can measure their impact by the change in the number of copyright-infringement complaints they receive under the terms of the *Digital Millennium Copyright Act* (DMCA). A number of universities report major reductions in these complaints after installing network-filtering technologies. For instance, Wittenberg University in Ohio estimates that its DMCA complaints dropped from 50 per year to about three after installing a network-filtering technology from Audible Magic Corporation. The University of Florida reports a drop from approximately 50 copyright-violation complaints per month to zero after deploying a network-filtering system now sold by Red Lambda, Inc. The University of Portland installed a network-filtering system two years ago, and currently blocks millions of copyright-violating files per month, resulting in a 70 percent reduction in DMCA complaints. Campuses using traffic-shaping technologies alone do not report experiencing as significant a reduction in DMCA complaints.

Do technologies to reduce illegal filesharing affect the speed and reliability of campus networks? Campus networks can be relatively complex, and must be able to transmit large amounts of data for research and educational purposes without major delays. Most universities agree that traffic-shaping technology improves, rather than harms, the performance of their networks by giving preference to digital traffic from classrooms and labs during peak usage hours and controlling large-scale characteristics of network transmission. In fact, a number of universities have been able to delay expensive upgrades to their network infrastructure because of traffic-shaping systems. However, there is some argument over whether network-filtering technology has a degrading effect on a network. Some universities have argued that it will slow down network speeds and reduce the reliability of the network. Others report that network-filtering systems increase the speed of their network for legitimate transmissions by eliminating large amounts of illegal usage, thus freeing up network resources. After installing network-filtering systems, Wittenberg University experienced a 63 percent reduction in network traffic, the University of Florida experienced a 40 percent reduction of inbound traffic and an 85 percent reduction of outbound traffic, and the University of Portland experienced at least a 50 percent reduction in overall network traffic. The experiences of campuses that are currently deploying both traffic-shaping and network-filtering technologies will help clarify the impact they have on network performance. Realistic testing with scientific metrics, as is being performed at Illinois State University, will also yield valuable data for evaluating these claims.

Do network-filtering technologies interfere with legitimate uses of campus networks? Since network-filtering technologies aim to specifically identify copyright-infringing content in data transmissions, there is a concern that they may incorrectly identify legitimate content that happens to be transmitted by peer-to-peer (P2P) filesharing protocols, and thus interfere with educational or research uses of the network. BitTorrent, a popular protocol for transferring large files, is used to illegally transfer copyrighted movies, but it is also used to download copies of the freely distributed Linux operating system, transfer satellite photos from NASA's Visible Earth website, and exchange many other legal files. The OCKHAM Initiative, a collaboration among Emory University, the University of Notre Dame, Oregon State University, and Virginia Tech, recently received a grant from the Na-

tional Science Foundation (NSF) to use P2P filesharing protocols to promote digital libraries for research and educational purposes. And Pennsylvania State University has developed and begun using LionShare, a legal and secure peer-to-peer filesharing program to transfer academic and personal files among institutions around the world. If network-filtering systems incorrectly identify these legitimate network transmissions as copyright-infringing, they would interfere with appropriate and necessary usage of campus networks and prevent educational and research activities. This issue is another area in which realistic testing with scientific metrics in the vein of the Illinois State University Digital Citizen Project can provide important data.

Are anti-illegal-downloading technologies vulnerable to hackers or other technological counter-measures? There is a concern among universities that network-filtering technologies may be quickly defeated by hackers, both on and off campus. Encrypting copyright-infringing files before they are transmitted may circumvent the detection step of network-filtering systems and allow users to continue illegal filesharing in spite of the installation of these technologies. While it is clear that any technological system is ultimately vulnerable to continual technological advances, understanding the ways in which network-filtering systems can be kept updated to respond to technological challenges will be important for evaluating the long-term utility of technical means to reduce illegal downloading. A useful parallel to this issue can be found in the growth and distribution of anti-virus and anti-spam software, the original versions of which would be entirely impotent in today's network environment. Continual updates in reaction to changes in the digital landscape have not only kept these programs effective, they have allowed them to improve their accuracy in eliminating viruses and spam and thus enhanced the utility of most networks on which they are installed. No responsible network administrator would today operate a system without anti-virus and anti-spam technology installed.

Do technologies to reduce illegal downloading compromise privacy of networks? Privacy on computer networks is a significant concern, and to the extent that it is compatible with legal usage it must be protected. Many universities are concerned that the component of network-filtering systems that identifies copyrighted material violates the privacy of users of the network, by more closely examining the content of their transmitted files. It is important to understand the methods by which these technologies identify copyright-infringing files, and whether these methods are more invasive to privacy of transmissions than other network maintenance operations, such as filtering e-mail for spam and examining downloaded files for possible viruses or computer worms. University witnesses at the hearing can provide insight about privacy concerns that may have arisen on their campuses when they deployed network-filtering technologies.

5. Background

Definitions and technical background

"Illegal filesharing" is a broad term for the digital distribution of files that contain copyright-protected material, such as music, movies, and some software. Illegal filesharing is usually accomplished with computer programs that create peer-to-peer (P2P) network connections linking many individual computers. A variety of P2P programs, such as Kazaa, LimeWire, eDonkey, and Morpheus are available for free download from their distributors' websites.

After a user installs a P2P program (called a "client application") onto their computer, he or she runs the application to connect to the computers of other users of that particular P2P software. The client application allows users to "share" files located on their computer hard drives. Once users make files available for sharing with each other, anyone who uses the same software to connect to the P2P network may locate and download desired files easily and at no cost. For example, a user of the LimeWire client application can directly access files saved on another LimeWire user's computer hard drive. Alternatively, a user can search for a particular file name, such as an MP3 song title, across all the computers connected to the LimeWire network, and then download a copy of that file onto his or her computer.

It is important to note that downloading music, movies and software over the Internet is not itself illegal, as long as users pay legal fees. For instance, Apple's iTunes Store allows users to legally purchase and download music for their iPod player, and services such as MovieLink and CinemaNow allow users to buy and download movies. There are also legal downloading sites for college and university students that are supported by advertising revenue or blanket subscription fees, such as Ruckus and Cdigix. However, using programs such as LimeWire to share

copyrighted material does not involve any royalty payment to the copyright owner, and is therefore illegal.

Impact on college and university networks

Illegal filesharing has become common at many colleges and universities across the country. According to a 2006 survey by the University of Richmond's Intellectual Property Institute, 34 percent of college students illegally download music from P2P networks. NPD Group, a leading entertainment research firm, found in a recent survey that more than two-thirds of music acquired by college students was obtained illegally, and that students are more than twice as likely as the general population to use P2P networks to download music. A 2005 study by L.E.K. Consulting found that 44 percent of U.S. losses to the movie industry from illegal filesharing were due to college students.

Under the "safe harbor" provisions of the 1998 *Digital Millennium Copyright Act* (DMCA), colleges and universities are not liable for copyright violations committed using their networks, as long as they cooperate with copyright holders who file complaints that their copyrighted material is being illegally transmitted over the campus network. Over the past two years, the music industry has sent almost 60,000 copyright-infringement notices to over 1,000 schools. This has created a significant administrative burden for the schools to process and respond to these claims. In addition, over 1,000 lawsuits have been brought against students at over 130 schools, and the cost of dealing with these claims can be quite high.

Illegal filesharing has had a major impact on the performance of campus networks. Shortly before the University of Florida deployed its network-filtering system, its dormitory network was at 95 percent of total transmission capacity. Prior to installing its network-filtering system, the University of Portland found that its network was transmitting files at 100 percent capacity. Many other campuses face a similar problem with increased campus demand for network access, and a number are finding that illegal filesharing is an unexpectedly large fraction of this demand. This has important consequences for campus decisions about the appropriate level of resources to invest in network expansions and upgrades.

Technological measures to prevent illegal filesharing

Colleges and universities can take a number of technological steps to help reduce illegal filesharing on their campus networks. These generally fall into two categories of technologies that can be installed on the campus network. The first category encompasses hardware and software systems known as "traffic shapers," which modify the rate at which certain files are transmitted over the network. Traffic-shaping systems prioritize the transmission speed of files based on a number of factors, such as where on the network the transmitted files originate (files from laboratory computers may receive faster transmission than those from dorm computers) or what software program is sending the files (files from known research software may be given faster transmission than data from games or other entertainment software). Traffic-shaping systems can also establish a maximum data transmission amount per day for users, so that users who "hog" transmission time can be prevented from overusing the network. While traffic-shaping systems do not specifically identify or target files that contain copyrighted material, they can reduce the flow of data to and from computers that tend to transmit or receive copyright-infringing transmissions, making illegal filesharing slower and more difficult. According to a 2005 survey by EDUCAUSE, almost 90 percent of campuses use some form of traffic-shaping technologies on their networks. Traffic-shaping products include Packeteer's PacketShaper, Allot Communication's NetEnforcer, and APconnections' NetEqualizer.

The second category of technologies available to campus networks to reduce illegal filesharing encompasses systems known as "network filters". These technologies use a variety of techniques to more closely examine transmissions on the network and specifically determine whether they contain copyrighted materials. They can generally be configured to either block the transmission of files that are found to contain these materials, or simply to log the infringing transmission and send warning notices to the user(s) involved. One of the methods employed by network-filtering technologies to detect copyrighted material is known as "fingerprinting," in which various characteristics of music tracks and movies (a "fingerprint" of the content) are stored in a database, and transmitted files are compared against this database to detect a match. A second method is based on analyzing the transmission patterns of data on the network and statistically comparing them with previously identified infringing network traffic. Network-filtering systems are not yet widely deployed by colleges and universities, although a growing number of schools are beginning to

adopt them. Network-filter products include Audible Magic's CopySense, Red Lambda's cGRID::Integrity, and SafeMedia's Clouseau.

Reactions from the university community

Most colleges and universities have embraced the adoption of traffic-shaping technologies. Their use of these systems is motivated partly by concerns about illegal filesharing and partly by the desire to make their networks more efficient. Many campuses have responded to the illegal filesharing issue with educational and awareness campaigns for their students, to teach them that filesharing using most free P2P software applications is illegal and could expose them to legal action. A smaller number of campuses (roughly 100 by the end of 2006) have begun providing legal alternatives for downloading music and movies. These legitimate services include Ruckus, Cdigix, and Napster, and are funded either by advertising revenue, flat student fees per semester, or other financing models. Education campaigns often include a component to teach students who are using P2P applications for illegal filesharing about the existence of these legal sites.

In contrast to attitudes towards traffic-shaping systems, education, and legitimate download services, many universities have raised objections to installing network-filtering technologies. These objections are based on policy, financial, and technical rationales, and have spurred a significant debate on the issue of the appropriate role for network-filtering systems in dealing with illegal downloading.

Policy objections to network-filtering systems are based on arguments that their use violates privacy, by inspecting network transmissions too closely. There is also an argument that network-filtering systems compromise academic freedom, by blocking or impeding the free transmission of data. These policy issues, while valid, must be considered in the context of other network-management policies in place on virtually all campus networks, including the use of anti-spam and anti-virus filters, which examine the content of transmitted files for unwanted commercial content (spam) or malicious software (viruses and worms). If the behavior of anti-spam and anti-virus software is not considered invasive of privacy or counter to academic freedom, then to the extent that network-filtering systems examine content in a similar fashion, they should not be considered so either.

Financial objections to network-filtering technologies generally involve concerns that it would be too expensive to purchase systems with sufficient capability to effectively reduce illegal filesharing on campus networks, and/or that it would be too expensive to pay for maintenance and upgrades to these systems. In addressing this issue, it is useful to consider the relative costs campuses currently pay for their network management, and place the cost of network-filtering systems in this context. While campuses differ, in the case of many campuses using network-filtering systems, the costs associated with these technologies are significantly less than that of other network management activities. In addition, network-filtering systems can relieve pressure on campus networks clogged with a mix of legitimate and illegitimate traffic, and thus eliminate or defer the need for expensive network-expansion projects. For example, the University of Florida was able to defer a $2 million network upgrade for over two years by installing a network-filtering system and reducing a large amount of network traffic that was determined to be illegal. Wittenberg University estimates that it saves between $20,000 and $25,000 annually on network usage because of its network-filtering system. Campuses also realize savings by not having to process as many DMCA complaints: the University of Florida saved roughly 3000 work-hours in the first year after installing its system, and Wittenberg University estimates it eliminated 90 percent of its complaint-processing time (roughly 45 work-hours per year) by using its network-filtering technology.

Finally, technical objections to network filters are grounded in the argument that they are imperfect, and do not detect and stop all illegal filesharing on a network. The objections also include concerns that network-filtering systems will be defeated by technical attacks, such as a move to encrypted data transmission for illegal filesharing or other work-arounds. While these systems are indeed imperfect in the sense that they do not prevent 100 percent of illegal transmissions, an important analogy can be made to the adoption and deployment of the first firewalls, spam filters and virus filters, which were and continue to be imperfect technologies, yet today form a critical digital defense across campus and commercial networks that no responsible network administrator would fail to employ. An adoption standard based on technical perfection is inconsistent with other technology adoption policies and is ultimately counter-productive.

Chairman GORDON. This hearing will come to order, and good afternoon to everyone. Welcome to today's hearing entitled *The Role of Technology in Reducing Illegal Filesharing: A University Perspective.* Today we are going to be addressing the issue of illegal filesharing on university computer networks. This practice, which is also known as digital piracy, is costing the entertainment industry billions of dollars and thousands of jobs.

I would also note that illegal filesharing isn't just about royalty fees. It clogs campus networks and interferes with the educational and research mission of universities. It wastes resources that could have gone to laboratories, classrooms, and equipment, and it is teaching a generation of college students that it is all right to steal music, movies, and other content because it is easy to download them on the Internet. That is wrong, and it needs to be stopped.

Our committee is not the first to address this issue. Under the leadership of my friend Lamar Smith the Judiciary Committee held a series of hearings on this topic in the last Congress. The Education Committee has also held a hearing on this issue. However, those hearings focused on the legal and regulatory structure as was appropriate given the jurisdiction of the Committees. The focus of today's hearing is on technology to help prevent illegal filesharing.

In today's digital world we generally rely on technology to combat illegal activities. It is illegal to send spam or to hack into a system to steal data. And though regulations attempt to stop these illegal activities, regulations alone are not enough. Systems from large corporate networks to home desktop computers use anti-spam and anti-virus software firewalls.

Do these technologies stop all illegal activities? Of course not, but they do prevent the bulk of bad things from happening, and the technologies have improved even as the sophistication of the spammers and hackers has increased. The Science and Technology Committee has a long history of holding hearings and moving legislation about technologies that are used to combat these illegal activities.

I believe the case of illegal filesharing is exactly the same. We can't rely on laws and regulations alone to fix the problem. Technology will be the first line of defense, and I am hopeful that our work here will contribute to the beginning of real action on this problem. I don't want to be holding this same hearing in the 111th Congress.

Our witnesses will focus on the use of technology to combat illegal filesharing. Some of them will discuss how their campuses decided to use technology to reduce digital piracy. I hope to learn about their experiences with these technologies and how well they have worked. I am also interested in learning about the technologies themselves; how they stop copyrighted files from being illegally shared and what technical issues there may be for implementing them on campus networks. And I am looking forward to hearing about an important cooperative project between higher education and the entertainment community to rigorously test and evaluate these technologies in an objective, scientific manner.

I want to thank our panelists for taking time from their busy schedules to appear before us today. One of our nation's greatest strengths is our education system, and America's universities are

the envy of the world. Their mission is to educate students, and they should not condone or look the other way when their computer networks are used as clearing houses for digital piracy and illegal filesharing. Universities do not condone piracy of computer software, textbooks, or academic research articles, and they should not treat entertainment intellectual property any differently.

It is my hope that by working together we can fix the problem of digital piracy on our campuses.

[The prepared statement of Chairman Gordon follows:]

PREPARED STATEMENT OF CHAIRMAN BART GORDON

Good morning. Welcome to today's hearing entitled *"The Role of Technology in Reducing Illegal Filesharing: A University Perspective."*

Today we are going to be addressing the issue of illegal filesharing on university computer networks. This practice, which is also known as digital piracy, is costing the entertainment industry billions of dollars and thousands of jobs. Many of the people affected by it are my constituents, who live near and work in Nashville, the recording capital of America. They are the ones who first brought this issue to my attention.

I would also note that illegal filesharing isn't just about royalty fees. It clogs campus networks and interferes with the educational and research mission of universities.

It wastes resources that could have gone to laboratories, classrooms, and equipment. And it is teaching a generation of college students that it's all right to steal music, movies, and other content, because it's easy to download them on the Internet. That's wrong, and it must be stopped.

Our committee is not the first to address this issue. Under the leadership of my friend Lamar Smith, the Judiciary Committee held a series of hearings on this topic in the last Congress. The Education Committee has also held a hearing on this issue. However, those hearings focused on the illegality and regulatory structure, as was appropriate given the jurisdiction of those Committees. The focus of today's hearing is on technology to help prevent illegal filesharing.

In today's digital world, we generally rely on technology to combat illegal activities. It's illegal to send spam or to hack into a system and steal data. And though regulations attempt to stop these illegal activities, regulations alone are surely not enough. Systems from large corporate networks to home desktop computers use anti-spam and anti-virus software and firewalls.

Do these technologies stop all illegal activities? Of course not. But they do prevent the bulk of bad things from happening. And the technologies have improved, even as the sophistication of the spammers and hackers has increased. The Science & Technology Committee has along history of holding hearings and moving legislation on technologies that are used to combat these illegal activities.

I believe the case of illegal filesharing is exactly the same. We can't rely on laws and regulations alone to fix the problem. Technology will be the first line of defense. I'm hopeful that our work here today will contribute to the beginnings of real action on this problem. I don't want to be holding this same hearing in the 111th Congress.

Our witnesses will focus on the use of technology to combat illegal filesharing. Some of them will discuss how their campuses decided to use technical methods to reduce digital piracy, and I hope to learn about their experiences with these technologies and how well they have worked.

I am also interested in learning about the technologies themselves—how they stop copyrighted files from being illegally shared, and what technical issues there may be for implementing them on campus networks.

And I am looking forward to hearing about an important cooperative project between higher education and the entertainment community to rigorously test and evaluate these technologies in an objective, scientific manner.

I want to thank our panelists for taking time from their busy schedules to appear before us today.

One of our nation's greatest strengths is our educational system, and American universities are the envy of the world.

Their mission is to educate students, and they should not condone or look the other way when their computer networks are used as clearinghouses for digital piracy and illegal filesharing. Universities do not condone the piracy of computer software, textbooks, or academic research articles, and they should not treat entertainment intellectual property any differently.

It is my hope that by working together we can fix the problem of digital piracy on campuses.

Chairman GORDON. And now I would like to yield to my friend, Mr. Hall.

Mr. HALL. And I assure you that I will call a hearing in the 111th if we need to, and I will confer with you in the kind of manner that you have with me, and I thank you for it.

Thank you, Chairman Gordon, for convening this very Full Committee hearing today. I would like to echo your welcome to our distinguished panel today, and I thank all of you for taking time to come to Washington to discuss how we can reduce digital piracy.

The breadth of experience and expertise here today I think is going to get us a long way in understanding the problem of copyright infringement and hopefully eliminate some of the next steps for the community.

In particular I would like to welcome Dr. Greg Jackson, the Chief Information Officer of the University of Chicago, and former Director of Academic Computing for the Massachusetts Institute of Technology. Dr. Jackson has also served on advisory boards for major information technology industry firms and helped usher in the next generation of Internet technologies with the National Lambda Rail and Internet 2 and I thank you, Dr. Jackson, and I look forward to hearing from you and all of your talented colleagues here today.

Piracy of digital available media has become a large concern as more and more intellectual and creative works are available in easily transferred digital format and access to high bandwidth networks has spread. High-speed Internet connections used to be limited to major universities and government research labs. Now, relatively cheap broadband access is available, including over 50 million residential high-speed connections. Through this combination illegal filesharing of music, movies, software, and other contents is easier than ever, literally at the click of a button.

This rampant disregard for copyright law absolutely needs to end. A number of other committees have set, have met to discuss aspects of this problem. The hearing today will examine for us one detail of the larger intellectual property enforcement debate, focusing on the efficacy of technological solutions to stopping illegal filesharing.

Colleges and universities hold a unique perspective being both creators of intellectual property, Internet service providers to a large and technically savvy group of students and staff, and custodians of some of the fastest cutting-edge networks in the Nation. From reading our witnesses' testimony, it is clear that no single silver bullet solution is available to stop unauthorized distribution of digital media while allowing authorized traffic.

The variety of campus network needs and policies with respect to the proper role of the institution in policing users leads to a highly diverse environment. However, recent work and cooperation among higher education, copyright holders, and technology companies has helped build an understanding of these varied requirements and given us insight into how we might proceed in the end. The technologies we will discuss today are going to form part of a larger anti-piracy solution that also includes legal alternatives,

education, and adequate protections of privacy and consumer rights.

And if I have any time left I yield to the gentleman, Mr. Sensenbrenner.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF REPRESENTATIVE RALPH M. HALL

Thank you, Chairman Gordon, for convening this Full Committee hearing today.

I'd like to echo your welcome to our distinguished panel today. Thank you all for taking the time to come to Washington to discuss how we can reduce digital piracy. The breadth of experience and expertise here today will get us a long way in understanding the problem of copyright infringement and hopefully illuminate some next steps for the community.

In particular, I'd like to welcome Dr. Greg Jackson, the Chief Information Officer of the University of Chicago and former Director of Academic Computing for the Massachusetts Institute of Technology. Dr. Jackson has also served on advisory boards for major IT industry firms and helped usher in the next generation of Internet technologies with National LambdaRail and Internet2. Thank you Dr. Jackson, I'll look forward to hearing from you and all of your talented colleagues here today.

Piracy of digitally available media has become a large concern as more and more intellectual and creative works are available in easily-transferred, digital format and access to high bandwidth networks has spread. High speed Internet connections used to be limited to major universities and government research labs. Now, relatively cheap broadband access is available, including over fifty million residential high speed connections. Through this combination, illegal filesharing of music, movies, software, and other content is easier than ever—literally at the click of a button. This rampant disregard for copyright law needs to end.

A number of other committees have met to discuss aspects of this problem. This hearing will examine one detail of the larger intellectual property enforcement debate, focusing on the efficacy of technological solutions to stopping illegal filesharing. Colleges and universities hold a unique perspective, being both creators of intellectual property, Internet service providers to a large and technically savvy group of students and staff, and custodians of some of the fastest, cutting edge networks in the Nation.

From reading our witnesses testimony, it is clear that no single, silver-bullet solution is available to stop unauthorized distribution of digital media while allowing authorized traffic. The variety of campus network needs and policies with respect to the proper role of the institution in policing users leads to a highly diverse environment. However, recent work and cooperation among higher education, copyright holders, and technology companies has helped build an understanding of these varied requirements and given us insight into how we might proceed. In the end, the technologies we'll discuss today will form part of a larger anti-piracy solution that also includes legal alternatives, education, and adequate protections of privacy and consumer rights.

Chairman GORDON. I was going to suggest that. Mr. Sensenbrenner has an appointment to chew someone out, and so we don't want to stand in his way, and we would like for him to——

Mr. SENSENBRENNER. It is the State Department on issuing passports. So there is a big problem with that.

First of all, I thank both the Chair and the gentleman from Texas for yielding.

When I was the Chair of the Judiciary Committee, I was really an intellectual property hawk, and I was the one that directed Congressman Smith to have the series of hearings in the last Congress relative to the copyright law and the enforcement of the copyright law.

This hearing closes the loop on this, because obviously we are never going to be able to get 100 percent enforcement given the massive popularity of the Internet and the new technologies for filesharing, and that is why the technologies are important to be able to prevent this from happening in the first place.

I am a graduate of Stanford University. So is my son, and when I went out to visit my son during his time out at Stanford, I frequently checked in with the front office, and one of the things that I talked about there was the problem of filesharing on university campuses. This was several years ago, and at that time the estimate was given to me that about 80 percent of the broadband that the university purchased, again, with the money that came from tuition and elsewhere, was used for filesharing, and only 20 percent was being used for legitimate research of other academic purposes.

This is a staggering figure, and to say that filesharing on university campuses does not drive up the cost of education is just flat out false. And the more we can do to have the technology to prevent this from happening in the first place, the better off the kids who don't fileshare will be in terms of not seeing one tuition increase piled on top of another tuition increase, and in the case of public universities, administrators having a good go at the legislature to get more taxpayers' dollars to be used to pay for this.

So I welcome this hearing today. I am sorry I have to go leave to chew the Director of Counselor Affairs out, but anybody who wants to travel overseas pretty soon and who doesn't have a passport yet, will know that I am doing the Lord's work there while you are doing the Lord's work here. So thank you.

Chairman GORDON. Thank you, Mr. Sensenbrenner. We should have called you as a witness.

If there are other Members who wish to submit additional opening statements, your statements will be added to the record.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF REPRESENTATIVE EDDIE BERNICE JOHNSON

Thank you, Mr. Chairman.

I would like to welcome here today the witnesses for today's hearing to explore technologies used by colleges and universities to reduce copyright-infringing filesharing on campus.

Universities historically have upheld strict standards in terms of ethical conduct, opposing plagiarism, and supporting moral values when it comes to the process of research and higher education.

Again, universities are positioned to take a leadership role in the practice of reducing illegal mass copying of music and videos in which it is against the law to reproduce and share the files.

Always at the cutting edge of technology policy discussions, the Committee on Science and Technology is eager to learn more about current best-practices on campus. We want to hear examples of excellence in protecting the copyrights of music and videos on campus.

Such technologies save the music and movie industries from costly losses due to illegal filesharing, and they enforce current copyright laws.

While these technologies have great potential for widespread adoption and use, they also have limitations. The Committee hopes to hear more about these limitations and how they can be overcome.

Other pertinent issues include whether the technologies compromise the privacy of campus computer networks and otherwise interfere with legitimate uses of campus computer networks.

Again, welcome to today's witnesses. Thank you, Mr. Chairman. I yield back.

[The prepared statement of Mr. Carnahan follows:]

PREPARED STATEMENT OF REPRESENTATIVE RUSS CARNAHAN

Mr. Chairman, thank you for hosting this hearing to explore approaches to the reduction of illegal filesharing on the campus networks of universities around the country.

Copyright-infringing filesharing costs the movie, music, and software industries hundreds of millions of dollars each year, and I look forward to examining ways that Congress can help to counteract this worrying trend.

Numerous studies by intellectual property and consulting firms over the past few years have shown that college students account for a disproportionately large percentage of illegal downloads on peer-to-peer networks. Increasingly, the high-speed Internet networks provided by universities for the purposes of education and research are becoming the domains of digital piracy and illicit filesharing by students.

Today's hearing focuses on the important task of bolstering the technology available to universities for controlling the copyright-protected material being transmitted across their campus networks. I am eager to hear our witnesses' assessments of the counter-measures implemented thus far so that we can reflect on the successes and inefficiencies of the technologies and seek to make modifications for improvement. Your first-hand experiences are vital to protecting the copyrights of musicians, producers, and software engineers, as well as maximizing the performance of university networks.

To all the witnesses—thank you for taking time out of your busy schedules to appear before us today. I look forward to hearing your testimony.

[The prepared statement of Mr. Mitchell follows:]

PREPARED STATEMENT OF REPRESENTATIVE HARRY E. MITCHELL

Thank you Mr. Chairman.

I would like to extend a special welcome today to Dr. Adrian Sannier, Vice President and University Technology Officer at Arizona State University. Dr. Sannier made a special trip to Washington today to represent Arizona State University, a groundbreaking research university in my hometown of Tempe, AZ.

Dr. Sannier is an integral part of ASU's mission to become a "New American University" and as such and it does not surprise me to know that the University Technology Office is at the forefront of peer-to-peer filesharing issues.

The purpose of today's hearing is to learn about the experiences universities have had combating illegal filesharing on campus. Illegal filesharing on campus networks puts many of our universities in a unique position. Students disregarding copyright protections may be liable for legal action, an incentive for many universities to block filesharing on their networks and protect students. At the same time legal filesharing (such as research) should be allowed and privacy protected.

Many universities are in a difficult position when it comes to solutions for illegal filesharing and some have implemented technological measures to reduce copyright-infringing filesharing on their networks.

ASU is one of the first universities in the country to implement technology to track and block illegal filesharing and Dr. Sannier will share his insight about ASU's experience with Audible Magic Corporations's anti-piracy technology—from what has worked to the school's concerns about existing technologies.

I look forward to Dr. Sannier's testimony and learning about the experiences of other universities around the country.

I yield back the balance of my time.

Chairman GORDON. And now I would like to recognize Mr. Matheson to introduce our first witness.

Mr. MATHESON. Well, thank you, Chairman Gordon, and I do want to introduce a constituent of mine, Dr. Charles Wight from the University of Utah. He has been a member of the faculty at the University of Utah since 1984, and he has many roles he has taken there, but among the many roles he serves as Associate Vice President for Academic Affairs and Undergraduate Studies. And in this role he is responsible for the university's continuing education unit, its general education program, and for development of policies for educational technology and online courses.

He serves on the university's academic leadership team and assists the Chief Information Officer, Dr. Steven Hess, in the development of institutional policies regarding institutional data access and security. And in 2001, he chaired a committee that wrote the current institutional policy governing copyright ownership for works created using resources of the University of Utah.

So I want to welcome him as a witness, and Mr. Chairman, I will yield back.

Chairman GORDON. Thank you very much, and our second witness is Dr. Adrian Sannier, the Vice President and University Technology Officer at Arizona State University, which is in the district of Mr. Harry Mitchell, and Mr. Mitchell had a conflict, but he sends his best, and I understand you are going to be meeting with him later. He is another valued Member of this committee.

And our third witness is Mr. Vance Ikezoye, President and CEO of Audible Magic Corporation of Los Gatos, California.

Our fourth witness is Ms. Cheryl Elzy, the Dean of University Libraries at Illinois State University and a member of the management team of the Digital Citizen Project.

And Mr. Hall has already introduced the Republican witness today, and so we are all glad you are here. As our witnesses know, your statements will be made a part of the record, and we hope that you can summarize. We try to keep it within five minutes, but we want to be sure that you feel comfortable getting your full point.

And then we will introduce our Members for five minutes. So we will now start with Dr. Wight.

STATEMENT OF DR. CHARLES A. WIGHT, ASSOCIATE VICE PRESIDENT FOR ACADEMIC AFFAIRS AND UNDERGRADUATE STUDIES, UNIVERSITY OF UTAH, SALT LAKE CITY

Dr. WIGHT. Mr. Chairman, Members of the Committee, I am pleased to appear today to share some of the experiences of the University of Utah in reducing illegal peer-to-peer sharing of music and video files.

My name is Chuck Wight, and I serve as Associate Vice President for Academic Affairs and Undergraduate Studies at the University of Utah.

First of all, I want to stress that respect for copyrights lies at the heart of what universities do. Students and faculty enjoy the protection of intellectual property that we create every day through scholarly research. As teachers, we enjoy special privileges from the Doctrine of Fair Use, which permits limited use of copyrighted materials for non-profit educational purposes.

Therefore, when members of our community abuse copyrights of others, whether it is plagiarism or through peer-to-peer filesharing, we take this very seriously.

At the University of Utah we have adopted a two-pronged approach to reducing illegal peer-to-peer filesharing. First of all, we continuously monitor our networks to identify high bandwidth users in all areas of the campus network. Each week every local area network manager receives a report of the top talkers on his or her local area network. Each LAN manager is responsible for assessing whether the high bandwidth activity is an appropriate use of university resources, and if not, that person is responsible for correcting the situation.

In the part of our network that serves the student residences, we run the Audible Magic software, which monitors network traffic to detect and block the transmission of copyrighted works that are

registered with Audible Magic. These are mostly music recordings and movies.

In addition, we automatically terminate network access to any student computer that has a total volume of outgoing network traffic that exceeds two gigabytes in a single day. Whenever this happens, someone from our information security office follows up with the user to determine whether or not the network activity was appropriate. That person then takes action to either restrict the activity or to allow it to continue.

This two-pronged approach to the peer-to-peer filesharing problem has been very successful for us. We reduced the number of DMCA copyright abuse notices from RIAA, MPAA, and others by more than 90 percent. We currently deal with only two or three notices per week. After implementing this strategy about three years ago, the university saved about $1.2 million per year in Internet bandwidth charges.

In addition, we saved an estimated $70,000 per year in personnel costs that would have otherwise been required to investigate and respond to copyright abuse complaints. Every time our information security office investigates a valid complaint or finds an instance of illegal filesharing activity, the user must agree in writing to abide by the university's acceptable use policy in order to have his or her network access restored. The rate of repeat offenses is low. In more than ten years there have been only three instances where a user's network access was permanently revoked.

It is important to realize that there is no software or other network monitoring technology that can identify illegal transmission of copyrighted material with 100 percent reliability. Port shifting and encryption are just two of the many effective strategies that peer-to-peer filesharing programs use to overcome almost any technology solution to this problem.

That is why it is important to use multiple strategies, for example, Audible Magic combined with network traffic volume monitoring, for detecting suspected violations. It is also important for the university to contact users personally in each case to make a detailed assessment of the situation.

Our approach is largely, though not 100 percent, effective for reducing illegal filesharing activities on our campus. It allows us to block some content automatically, and it allows us to ensure that our network bandwidth resources are used appropriately, while at the same time respecting the privacy of individual users.

Thank you.

[The prepared statement of Dr. Wight follows:]

PREPARED STATEMENT OF CHARLES A. WIGHT

Mr. Chairman and Members of the Committee, I am pleased to appear today to share some of the experiences of the University of Utah in reducing the illegal sharing of digital copyrighted materials. My name is Charles Wight, and I currently serve as Associate Vice President for Academic Affairs and Undergraduate Studies at the University of Utah. In this capacity I am responsible for, or I am otherwise engaged in, creating and implementing a wide range of university policies dealing with educational technology, online courses, Internet security, copyright policy, institutional data access, and student behavior.

Copyright law is essential to many of the core functions of universities. Faculty, staff and students enjoy protection of the intellectual property that is created every day through the process of scholarly research. Teachers also derive enormous benefit

from the doctrine of Fair Use (sections 107 through 118 of the Copyright Act, Title 17 of United States Code), which permits limited free use of copyrighted materials for nonprofit educational purposes. Therefore, we are concerned whenever members of our university community are engaged in activities that violate the copyrights of others.

The University of Utah employs two independent technology solutions on its campus network to address the problem of illegal filesharing. The first is continuous monitoring of network traffic to identify high-bandwidth users in all areas of campus. The second is a network monitoring program called Audible Magic, which detects and blocks transmission of unencrypted copyrighted music and video recordings from computers in the student residence halls. The decision to use these technologies for detecting suspected cases of copyright abuse through peer-to-peer filesharing was made by its Chief Information Officer, Dr. Stephen Hess, in consultation with the University administration and the University's Information Technology Council, a broadly based oversight committee composed of faculty and staff from all major areas of the campus. The University's Information Security Office (ISO) implements the policies.

The ISO network monitoring software automatically generates daily reports for the manager of each local area network (LAN), typically for a department or college within the university. The report lists all of the computers connected to that LAN for which the volume of outgoing network traffic exceeded one gigabyte (GB) over a 24 hour period. Each LAN manager is responsible for assessing the type of information being sent and whether the use of network resources is consistent with university policy and applicable laws. In most cases, the traffic is associated with legitimate teaching and research functions of the university. However, in some cases, LAN managers are able to identify computers that are transmitting large amounts of data inappropriately. It is the responsibility of the LAN manager to isolate the offending computer from the campus network and to contact the user or administrator of the machine to make a detailed assessment of the situation.

The ISO also runs Audible Magic network monitoring software in the local area network serving our student residence halls, where the potential for illegal filesharing is high. The software is designed to detect transmission of copyrighted materials registered with Audible Magic by looking for particular patterns of bits crossing the network, somewhat like software designed to detect computer viruses. Whenever Audible Magic detects the transmission of a protected work, the transmission is automatically reset, preventing the protected work from being shared. Additionally, network access is cut off automatically if the total volume of outgoing network traffic from a student computer in the residence halls exceeds two GB per day.

Currently, the ISO deals with suspected cases of abuse of network resources about two or three times each week. Approximately 70 percent of the instances occur in the area of our network that serves the student residence halls. If the ISO finds that a user violated the university's Information Resources Policy (*http://www.admin.utah.edu/ppmanual/1/1-15.html*), then the ISO representative reviews that policy with the user. The user must then provide a signed statement agreeing to abide by the policy as well as applicable federal and State laws. Only then is the user's access to the network restored. Students who violate the policy more than once are referred to the Dean of Students and the Student Behavior Committee for disciplinary action.

This two-pronged technology solution has been effective for minimizing the amount of illegal copyright violations on campus through peer-to-peer filesharing. In the past 10 years, there have been only three instances in which it was necessary to permanently revoke a user's access to the university network. Since we began using the Audible Magic network monitoring software more than two years ago, the number of copyright abuse notices received from the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) has declined by more than 90 percent. The strategy also pays financial dividends for the university. By focusing attention on high-bandwidth users, the University has saved enormous amounts of money that would have otherwise been required to build network capacity to support illegal activities. Our ISO currently spends only about three person-hours per week dealing with network abuse issues. Without the two technology solutions in place, it is likely that it would require at least one additional full-time employee to respond to complaints.

It is important to note that there is no software or other network monitoring technology that can identify illegal transmission of copyrighted material with 100 percent reliability. Audible Magic only detects transmission of works that are registered with the company. Furthermore, it cannot detect the transmission if the session is encrypted (e.g., with the BitTorrent peer-to-peer filesharing software). Moni-

toring network traffic volume can identify large bandwidth users, but does not necessarily indicate illegal activities. That is why it is important to employ at least two independent strategies (e.g., network traffic volume and Audible Magic) for detecting suspected violations. It is equally important to reserve judgment in each case until after making personal contact with the user or administrator of a suspect computer to assess whether or not the use of university network resources is appropriate.

In conclusion, the University of Utah currently employs a two-part strategy of monitoring local network traffic volume across its entire network and operating filesharing detection software in the local area networks serving the student resident halls. This strategy is largely, though not 100 percent, effective for identifying inappropriate peer-to-peer filesharing activities involving copyright infringement. The strategy protects the privacy of individuals while at the same time flagging suspicious activities electronically. When suspected cases of network abuse are detected, university officials follow up with individual computer users to determine whether or not the activity is appropriate, and they take any actions necessary to ensure that our network resources and the Internet are used responsibly.

BIOGRAPHY FOR CHARLES A. WIGHT

Professor Charles Wight has been a member of the University of Utah faculty since 1984. His primary academic appointment is in the Chemistry Department, where he and his research group perform research on the chemical reactions and combustion of high explosives and solid rocket propellants. Chuck is the Deputy Director of the University of Utah Center for Simulation of Accidental Fires and Explosions, a large multi-disciplinary center for high-performance computing and simulation. Chuck serves as Associate Vice President for Academic Affairs and Undergraduate Studies. In this role, he is responsible for operating the University's Continuing Education unit, its General Education program, and for development of policies for educational technology and online courses. He serves on the University's Academic Leadership Team and assists the Chief Information Officer, Dr. Stephen Hess, in the development of institutional policies regarding institutional data access and security. In 2001, Chuck chaired a committee that wrote the current institutional policy governing copyright ownership for works created using University of Utah resources.

Chairman GORDON. And Dr. Sannier, you are recognized.

STATEMENT OF DR. ADRIAN SANNIER, VICE PRESIDENT AND UNIVERSITY TECHNOLOGY OFFICER, ARIZONA STATE UNIVERSITY

Dr. SANNIER. Thank you, Chairman Gordon, Ranking Member Hall, and distinguished Members of the Committee for giving me this opportunity to describe for you Arizona State University's use of technology to reduce the incidence of copyright infringing filesharing on its campus networks.

My name is Adrian Sannier, and I am the University Technology Officer at Arizona State University responsible for the governance of the network, among other duties. As one of the Nation's largest universities with over 65,000 students attending its four campuses in the metropolitan Phoenix area, ASU provides its students, faculty, and staff with an extensive and evolving array of computing and communication services. These services have become a core enabler of the university's academic and research missions and will continue to do so in the foreseeable future.

To govern the legitimate use of these services, ASU has developed an acceptable use policy for its computing and communication services that expressly forbids their use to transfer or exchange files when that transfer or exchange would infringe on copyright. Users of the university's computing and communication services must electronically agree to this policy as a condition of connection. The policy explicitly forbids the use of university communications

or computing infrastructure for any unlawful communications, including threats of violence, obscenity, child pornography, copyright infringement, and harassing communications.

I am pleased to report that despite some reports to the contrary in the popular press, ASU has a relatively low rate of complaint about the illegitimate use of its network from copyright holders such as the RIAA. ASU's complaint rate, which is the number of individuals alleged to have distributed copyrighted content per thousand students, is less than half of one percent, the lowest among the 25 institutions for which the RIAA released data this past spring.

In a recent letter to university presidents around the Nation, the RIAA outlined a set of four best practices that they recommended that universities employ to prevent or reduce student exposure to lawsuits. ASU was an early adopter of these practices, and they are the cornerstones of our successful containment efforts.

The first recommended practice is education. ASU incorporates education about the illegitimate use of networks in our new student orientations, our residence hall orientations, and our twice yearly information security orientations.

The second recommended practice is to offer students a legitimate online service as an alternative to illegitimate filesharing. Beginning in July of 2005, ASU was an early adopter of one such service, a digital entertainment network designed specifically for college students known as Ruckus. ASU's subscription provides its students with downloadable access, legal downloadable access, to 2.75 million songs, full-length feature films, short-form video, sports clips, and music videos, as well as access to a social network site focused on the network.

The third recommended practice is to take appropriate disciplinary action when students are found to be engaging in infringing conduct online. And so in addition to sanctions available under applicable law, ASU, and regents' policy, ASU can impose temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, or ASU-administered computing rooms, services, or facilities in the event of infractions.

The RIAA's final recommendation encourages universities to implement technical solutions to restrict, filter, or curtail peer-to-peer filesharing. Any technical solution must balance the rights of copyright holders with the legitimate uses of the university's network and its users' expectations of privacy and academic freedom.

Beginning in December of 2000, ASU's first attempt at such a solution was a packet-shaping solution. The packet-shaping solution restricted the amount of bandwidth available to peer-to-peer filesharing to a portion of the network bandwidth so that we could contain how much filesharing was being done. But by 2006, the amount of illegitimate network traffic had grown so high that reinvesting in that solution, which had cost the university about $250,000, seemed the wrong alternative.

After evaluating several different products and approaches, we have finally settled on Audible Magic's CopySense Network Appliance. The CopySense product does not disable peer-to-peer networking services or restrict the bandwidth available to them. In-

stead, the CopySense Appliance treats copyrighted material as if it were a computer virus on a P2P network. It works by blocking the exchange of copyrighted content while allowing legitimate files to transfer unobstructed. While our technical team was skeptical of this approach at first, our initial tests convinced us that the CopySense approach would provide us with a viable solution.

We installed the CopySense solution in spring semester without fanfare. It was configured to reject any traffic identified as registered commercial music, likely commercial music, commercial film and TV, or likely commercial software, and it began rejecting about between five and 10 percent of the overall network bandwidth immediately, identifying that traffic as the exchange of copyrighted material.

Overall I would classify our adoption of CopySense as one of the easiest technical adoptions we have undertaken and that it has thus far caused very little disruption in our community.

The list price is just over $200,000, and so that as a pioneer reference account, we will probably end up spending closer to half of that for an implementation of ASU's scale.

While we at ASU are pleased with our new technical solution, we remain concerned about the potential for ongoing arms races. Peer-to-peer services have evolved to defeat counter measures before, and it would be foolhardy to think that they won't continue to do so. And as long as these arms races continue, universities will be called upon to continue to expend resources in the defense of copyright that they might spend otherwise.

We, therefore, applaud the progress that many in the market have made in developing new and more effective business models for the consumer-friendly distribution of electronic content and look forward to the day that these improved services make copyright-infringing file exchange unattractive to all but the fringe of our community.

Thanks again for this opportunity to share Arizona State University's experiences with you.

[The prepared statement of Dr. Sannier follows:]

PREPARED STATEMENT OF ADRIAN SANNIER

Thank you, Chairman Gordon, Ranking Member Hall, and other Members of the Committee for giving me an opportunity to describe for you Arizona State University's use of technology to reduce the incidence of copyright-infringing filesharing on its campus networks.

As one of the Nation's largest universities, with over 65,000 students attending its four campuses in the metropolitan Phoenix area, ASU provides its students, faculty and staff with an extensive and evolving array of computing and communications services. These services have become a core enabler of the University's academic and research missions.

To govern the legitimate use of these services, ASU developed an Acceptable Use Policy for its computing and communication services that expressly forbids their use to transfer or exchange files when that transfer or exchange would infringe on copyright. Users of the University's computing and communication services must electronically agree to this policy as a condition of connection. The policy explicitly forbids the use of university communications or computing infrastructure for any unlawful communications, including "threats of violence, obscenity, child pornography, copyright infringement and harassing communications."

I am pleased to report that, despite some news reports to the contrary in the popular press, ASU has a relatively low rate of complaint about the illegitimate use of its network from copyright holders such as the RIAA. ASU's complaint rate, which is the number of individuals alleged to have distributed copyrighted content

per thousand students, was only 0.52 percent, the lowest among the 25 institutions for which the RIAA released data this past Spring.

In a recent letter to University Presidents around the Nation, the RIAA outlined a set of four best practices that they recommend universities employ to prevent or reduce student exposure to lawsuits and/or *Digital Millennium Copyright Act* notices. ASU was an early adopter of each of these best practices, and they are the cornerstones of ASU's successful containment efforts.

The first recommended practice is to educate students about the do's and don'ts of downloading and copying music and other copyrighted works. ASU incorporates these topics as part of our new student orientations, our residence hall orientations and our twice yearly information security week orientations.

The second recommended practice is to offer students a legitimate online service, one that provides an inexpensive alternative to illegal filesharing. Beginning in July of 2005, ASU was an early adopter of one such service, a digital entertainment network designed specifically for college students known as Ruckus. ASU's subscription provides its students with downloadable access to 2.75 million songs, full-length feature films, short-form video, sports clips, and music videos, as well as access to a social network site focused on the network.

The third recommended practice is to take appropriate disciplinary action when students are found to be engaging in infringing conduct online. Under the terms of ASU's Acceptable Use Policy,

> *upon receiving notice of a violation, ASU may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings. A person accused of a violation is notified of the charge and has an opportunity to respond before ASU imposes a permanent sanction.*

In addition to sanctions available under applicable law and ASU and regents' policies, ASU may impose a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, ASU-administered computing rooms, and other services or facilities.

The RIAA's final recommendation encourages universities to implement a network technical solution to restrict, filter, or curtail peer-to-peer filesharing. Any technical solution must balance the rights of copyright holders with the legitimate uses of the university's network and its users' expectations of privacy and academic freedom.

Beginning in December of 2000, ASU's first attempt at a solution was a network monitoring solution from Packeteer. ASU used the Packeteer product to monitor network data streams and use the protocol information contained in the streams to prioritize traffic. This allowed ASU the amount of university bandwidth devoted to peer-to-peer traffic to be strictly limited. Over a five year period, ASU invested more than $250,000 in the installation and maintenance of this solution, which was purchased and maintained solely for its role in protecting the interests of copyright holders. In 2006, as the legitimate traffic volumes continued to increase, requiring a concomitant increase in investment in Packeteer, ASU began to look for a different solution.

After evaluating several different products and approaches, we have finally settled on Audible Magic's CopySense Network Appliance. The CopySense product does not disable peer-to-peer networking services or restrict the bandwidth available to them. Instead, the CopySense Appliance treats copyrighted material as if it were a computer virus on a P2P network. It works by blocking the exchange of copyrighted content while allowing legitimate files to transfer unobstructed. While our technical team was skeptical of the approach at first, our initial tests convinced us that the CopySense approach would provide us with a viable solution.

We installed the CopySense in spring semester without fanfare. It was configured to reject any traffic identified as registered commercial music, likely commercial music, likely commercial film and TV, or likely commercial software. It began rejecting about five percent of the overall network bandwidth immediately, identifying that traffic as the exchange of copyrighted material. Despite the interruption in network transmission, there was no noticeable increase in calls to our help desk, and we received no complaints about network performance for legitimate purposes attributable to the CopySense product.

Overall I would classify our adoption of CopySense as one of the easiest technical adoptions we have undertaken and that it has thus far caused very little disruption in our community.

The list price for the CopySense product at ASU's scale is just over $200,000, but ASU expects its costs this year, as a Pioneer Reference Account, to be closer to one-half that price.

While we at ASU are pleased with our new technical solution, we remain concerned about the potential for an ongoing "arms races." Peer-to-peer services have

evolved to defeat effective counter-measures before and it would be foolhardy to believe that no further evolution is possible. As long as this "arms race" continues, universities will continue to be called upon to spend scarce resources procuring and deploying the latest technical counter-measures and expending time and energy in the protection of copyright at the expense of the value-added application of emerging technologies to the core missions of the institution.

We therefore applaud the progress that Apple and others have made in developing new and more effective business models for the consumer friendly distribution of electronic content and look forward to the day that these improved services make copyright-infringing file exchange unattractive to all but the fringes of our community.

Thank you again for the opportunity to share Arizona State University's experience with you.

BIOGRAPHY FOR ADRIAN SANNIER

Dr. Adrian Sannier was recently named Vice President and University Technology Officer at Arizona State University. The former Stanley Professor of Interdisciplinary Engineering at Iowa State University's Department of Industrial and Manufacturing Systems Engineering, Sannier brings with him 17 years of experience in both the public and private sectors. At Iowa State, Sannier was one of the founders of the Human Computer Interaction program and, in addition to research and teaching, was Associate Director of ISU's Virtual Reality Applications Center. Research at VRAC focuses on the applications of immersive visualization and next generation human/computer interfaces to challenges in science, technology and the humanities. Prior to joining the Iowa State University faculty in 2001, Sannier was Vice President and General Manager of Engineering Animation, Inc., a leading provider of 3D computer graphics software. Sannier led a group of 200 programmers and artists, who created products for a diverse group of companies, from Mattel and Disney to Ford and General Motors.

Chairman GORDON. Thank you, and Mr. Ikezoye.

STATEMENT OF MR. VANCE IKEZOYE, PRESIDENT AND CEO, AUDIBLE MAGIC CORPORATION

Mr. IKEZOYE. Good afternoon, Chairman Gordon, Ranking Member Hall, and distinguished Members of the Committee. My name is Vance Ikezoye, and I am President and CEO of Audible Magic Corporation. Thank you for your invitation to appear today.

By way of background, Audible Magic provides solutions to identify and manage electronic media, including preventing its piracy. My testimony here today is intended to provide an overview of the technological aspects of this issue, not to advocate a specific public policy position.

Audible Magic has developed a technical solution called the CopySense Appliance. Our product provides universities the ability to automate the education process, and enforce network use policies related to copyright, while protecting students' privacy and academic access to technology.

We introduced this solution in late 2003, and to date we have over 80 customers worldwide. We have over 70 higher education customers that range in size from as few as 150 students to large public universities. Our experience has shown that the use of technology such as CopySense has significantly reduced piracy on campuses. On one college campus, we saw within one month an 80 percent decrease in total network traffic, a 71 percent decrease in the number of users of filesharing applications, and finally, the filesharing traffic itself dropped from 20 gigabytes per day to effectively zero in less than one week.

CopySense Appliance was designed to intelligently detect and manage copyrighted content transfers over public filesharing appli-

cations like BitTorrent and Gnutella. Using our copyright identification technology, the system matches unknown files transferred over known public peer-to-peer filesharing applications to a database of copyrighted materials that have been registered by the copyright owners.

Our design philosophy is based upon the belief that peer-to-peer technology is not the problem. Peer-to-peer filesharing networks are an efficient means to distribute legitimate materials such as Linux software or even promote local unsigned artist's music. However, it is the unauthorized transfers of copyrighted works, whose owners do not want their works copied, that is the problem.

Our product allows the technology to work for everyone. The system can be used to allow content owners, such as a local garage band, to designate their content to be freely distributed, while a major label could designate their content to be blocked from distribution. Our product ranges in price from $5,000 on a small network to about $100,000 for a larger university network, depending on the bandwidth managed.

I would like to highlight for the Committee the new capabilities introduced this year, which are specifically designed to support universities in their mission to educate students. The CopySense system provides universities the ability to influence student behaviors through a graduated series of student communication and sanctions. The CopySense system can detect student violations of the university's network policies, which can include using peer-to-peer applications to download copyrighted music or movies.

Upon detection of these violations, the system will communicate with the student by automatically redirecting the student's Internet browser to a university-maintained website. This website can be used to educate the student on their violation and the reasons why their behavior was inappropriate. These pages could even be used to administer a copyright lesson and test. Because the system triggers at the time of the violation, the system is able to leverage the teachable moment by immediately providing feedback to the student.

The system possesses a configurable point system that provides an escalation in notifications or sanctions. The system could be configured to direct communications privately to the student violating the school policy. Any other information or reports could be restricted from access by others. In this way the system can comply with most universities' privacy policies.

I would like to point out that no technology is or will ever be a 100 percent effective solution, no matter what the context. But I will also propose that a solution does not have to be 100 percent to be effective and to make a difference on campuses.

One issue we hear from larger universities is a concern that our technology cannot handle their high bandwidth networks. First, our technical system is not an inline device. If an inline device is not fast enough, or even worse fails, it can slow down or stop network traffic. The CopySense Appliance performs its matching activity in parallel with a real-time network traffic flow. The actual experience of our customers has been that the CopySense Appliance has no adverse impact on network performance.

Secondly, we often get questions about our effectiveness; how can we match and identify files quickly enough to stop the transmissions of offending files when the campus networks are so fast? We have designed a very sophisticated solution to these problems. Let me briefly explain both the concern and how we handle it.

Files transferred over networks are broken up into discreet chunks referred to as packets. In order to make a match, a portion of the file will need to be reassembled and a number of packets collected. At that point we can perform the match using our fingerprinting technology.

You might be thinking, this must take a long time, and so on high speed networks the system won't ever match a file before the offending file transfer has already occurred. Our technical approach isolates this problem to only the first time we see the file being transferred. The first time we encounter a file we have never seen before, we must go through the process of using our fingerprinting technology. However, once this occurs, we can associate the file with an identifier, which is like an ID number. This ID number can be read from the data transmission very quickly and in more than enough time to take action.

Can technology solve the problem of piracy of copyrighted works in every instance? Can technology clear all university and college campuses of illegal filesharing? Technology will never be the entire solution. Technology is just one of the essential tools to combat piracy on campuses and as the title of this hearing indicates technology can reduce the number of violations and play a major role in supporting universities' and colleges' efforts to address this most important issue.

[The prepared statement of Mr. Ikezoye follows:]

PREPARED STATEMENT OF VANCE IKEZOYE

Good afternoon, Chairman Gordon, Ranking Member Hall, and distinguished Members of the Committee. My name is Vance Ikezoye and I am President and CEO of Audible Magic Corporation. Thank you for your invitation to appear today to discuss the important issue of using technology to reduce digital copyright violations on university and college campuses.

By way of background, I am a co-founder of Audible Magic. I have a Bachelor's degree in Engineering from the University of California, Berkeley and a MBA from the University of Pennsylvania, Wharton School. My work experience includes 13 years at Hewlett-Packard. Audible Magic was founded in 1999 and is based in Los Gatos, California. We provide technologies, services, and easy-to-use solutions to identify and manage electronic media, including preventing its piracy. Our customers include legitimate peer-to-peer networks such as iMesh and Kazaa, and video sharing and social community sites like MySpace and Microsoft Soapbox. Artists, publishers and content owners desiring to protect or manage their copyrighted music, video or software register in Audible Magic's continually updated database. The electronic fingerprint and ownership information database currently exceeds five million works and is one of the largest collections of its kind in the world. My testimony here today is intended to provide an overview of the technological aspects of this issue, not to advocate a specific public policy position.

Audible Magic has developed a technical solution called the CopySense Appliance. Our product provides universities the ability to automate the education process, enforce network-use policies related to copyright, while protecting students' privacy and academic access to technology.

Technology's Effectiveness on Campuses

We introduced this solution in late 2003 and to date have over 80 customers worldwide including about 70 university and college customers. Our university customers span all corners of the United States and range in size from as few as 150 students to large public universities. In addition, we hope to soon have one of the

highest enrollment universities in the United States as a customer. Both private and public institutions use the CopySense Appliance as a solution to illegal peer-to-peer filesharing on campus. *Our experience in over 70 universities and colleges has shown that use of technology such as CopySense has significantly reduced piracy on campuses.* On one college campus, we saw within one month an 80 percent decrease in total network traffic, a 71 percent decrease in the number of users of peer-to-peer filesharing applications, and finally the peer-to-peer filesharing traffic dropped from 20 GB per day to effectively zero in less than one week.

The CopySense Appliance was designed to intelligently detect and manage copyrighted content transfers over networks by individuals using popular public filesharing applications like BitTorrent and Gnutella. Since 2003, we have continued to improve our product and have focused on developing features to support the needs of universities and other educational institutions. Our solution is a turnkey, hardware product that is easily installed on the network of a university and provides automated detection and enforcement of copyright policies that are defined by the university administration. I will talk later about the new features we have integrated which provide tools to support the education of students in this area of copyright.

Using our copyright identification technology, the system matches unknown files transferred over known public peer-to-peer filesharing applications to a database of copyrighted materials that have been registered by the copyright owners. Since we focus on known public peer-to-peer filesharing applications, private communications such as e-mail pass by unaffected.

Our design philosophy is based upon the belief that peer-to-peer filesharing technology is not the problem. In fact, peer-to-peer technology is powerful and will be utilized increasingly in mainstream applications in the future. Peer-to-peer filesharing networks themselves are an efficient means to distribute legitimate materials such as Linux software or even promote local unsigned artists' music. However, it is the unauthorized transfers of copyrighted works, whose owners do not want their works copied that is the problem.

Our product allows the technology to work for everyone. The system can be used to allow content owners, such as a local garage band, to designate their content to be freely distributed, while a major label or movie studio could designate their content to be blocked from distribution. All other content passes through unimpeded without affecting the network's performance or reliability.

Our product ranges in price from $5,000, on a small network, to $100,000 for a large university network, depending on the network bandwidth managed. Our customers have found that we can provide a cost-effective solution that can save them significant costs of bandwidth while providing better service to their users. As an example, one of our customers is a small technical high school, which uses a DSL connection, like many people have in their homes, and it found our product to dramatically improve its users' satisfaction in a cost-effective manner.

New Tools to Support Education of Students

I would like to highlight for the Committee the new capabilities of the CopySense Appliance, introduced this year, which are specially designed to support universities in their mission to educate students. The CopySense system provides universities the ability to influence student behaviors through a graduated series of student communications and sanctions. The CopySense system can detect students' violations of the university's network policies and apply automated sanctions to the violators, which are defined by the university administration. The university can configure the product to detect specific behavioral violations, which can include using peer-to-peer applications to download copyrighted music or movies.

Upon detection of these violations, the system will communicate with the student by automatically redirecting the student's Internet browser to a website which the university maintains. This website can be used to educate the student on their violation and the reasons why their behavior was inappropriate—these pages could even be used to administer a web-based copyright lesson and test. Because the system triggers at the time of the violation, the system is able to leverage the 'teachable moment' by immediately providing feedback to the student.

The system possesses a configurable point system that provides an escalation in the notifications or sanctions. As an example, if a student was a serious repeat offender, the system could block the student's web, e-mail, or Internet access for preset periods of time.

The system could be configured to direct communications privately to the student violating the school policy. Any other information or reports could be restricted from access by others unless configured and specified by the University. In this way the system can comply with most universities' privacy policies.

Concerns About Technical Effectiveness

Before I get into specific issues that are commonly brought up about network technologies, I would like to point out that no technology is or will ever be a 100 percent effective solution no matter what the context. But I will also propose that a solution does not have to be 100 percent to be effective and make a difference on campuses.

Our design principle is that the system should not be over-reaching. Adopting this design principle, by definition, says that our system will not be a 100 percent solution. As an example, we may not be able to identify or even detect 100 percent of the filesharing traffic on the network. In order to detect 100 percent of the traffic, our system would have to be installed on every segment and device on the network—and this could dramatically increase costs. However, as I suggest, if we focus on feedback in an effort to educate students, we might begin to achieve the end result of correcting improper behaviors.

A critical concern of any technology relates to privacy. We have designed the CopySense system so that it can be configured to restrict access to information in a manner consistent with a university's privacy policy. If so configured, the university could treat this system as a black box as they do their other network equipment. This black box operates automatically without access by unauthorized personnel. In this way, the system's educational features could be configured so that only the student is notified of detection of their inappropriate behavior.

The second aspect of the system design with respect to privacy is that the system matches only copyrighted items in a database that are transferred over known public filesharing networks. All other communications such as e-mail and web traffic go by unimpeded and without inspection. Our product operates in a manner similar to anti-virus products or even spam filters. Only our registry contains fingerprints of copyright works rather than fingerprints of viruses or spam.

From one perspective, our product is much less invasive from a privacy point of view than spam-filtering technology. Our product only detects the transfer of copyrighted works over public filesharing networks. Remember that these networks connect millions of anonymous strangers who are revealing the contents of their computers' hard drives; it is a question if there is even an expectation of privacy under these circumstances. Contrast that with spam-filtering technologies, which scan and intercept private e-mail communications between known individuals.

One issue we hear from larger universities is the concern that our technology cannot handle the high-bandwidth speeds that they have deployed on their campuses. First, from a network administrative point of view, our system is not an in-line device. In-line devices are problematic since all the data traffic needs to go through them. If the device is not fast enough or even worse, fails, it can slow down or stop network traffic. As a device that is not in-line, the CopySense appliance operates on the sidelines and performs its matching activity in parallel with the real time network traffic flow. The actual experience of our university customers has been that the CopySense appliance has no adverse impact on network performance.

Secondly, we often get questions about our effectiveness—how can we match and identify files quickly enough to stop the transmissions of offending files when the campus networks are so fast? We have designed a very sophisticated solution to this question. Let me briefly explain both the concern and how we handle it.

Files transferred over networks are broken up into discrete chunks referred to as packets. In order to make a match using our technology, a portion of the file will need to be reassembled and a number of packets collected and buffered. Our system in the course of its operation does this routinely. Once we collect and reassemble enough of the file, we can perform a match using our fingerprinting technology.

You might be thinking, "This must take a long time and so on high-speed networks the system won't ever match a file before the offending file transfer has already occurred." Our technical approach isolates this problem to only the first time we see the file being transferred.

The first time our product comes across a file we have never seen before, we must go through the process of collecting and analyzing the file using our fingerprinting technology. As one might guess, on high-speed networks it may happen too fast for our technology. However, after this initial experience with the file, we can associate the identity of the file with an identifier, which is like an ID number for files shared over these networks. This ID number can be read from the data transmission very quickly—in more than enough time to take action. We maintain a local list of these identifiers in every system installed. Thus in most cases, this list can be used to accurately match files transferred even over high-speed networks in plenty of time to react.

I also want to point out that our CopySense content identification solution has become the industry standard, not only in the university network community, but

in other technology settings, including legal peer-to-peer systems and user-generated content websites like MySpace, GoFish, and others. One of the many reasons why our technology has been adopted is because it is highly accurate.

A general concern raised about any network traffic analysis is the issue of encrypted filesharing networks. Encryption is a technique that is commonly used in electronic communications to scramble what would otherwise be an open, readable message. Encryption is most commonly used in financial transactions over the Internet, such as a credit card transaction, in order to protect the privacy and security of these transactions.

Peer-to-peer filesharing applications have adopted encryption, however, not to protect the privacy of the users, but to inhibit network management of peer-to-peer traffic and to prevent detection of illegal transfers of copyrighted-content files. The reality is that encryption technology can prevent the detection of content transfers at the file level such as that performed by our product. There are popular filesharing applications that use various levels of encryption today. However, even peer-to-peer filesharing applications that encrypt data often have some unique characteristics that identify the transfers. Our product deals with this by providing the university the ability to detect and block the use of encrypted peer-to-peer filesharing applications. This in combination with the educational features of the system is intended to discourage use of encrypted filesharing applications and migrate users back to unencrypted filesharing applications.

The term "darknet" generally refers to filesharing application networks that limit themselves to a local area such as a floor within a dorm. These darknets provide students a mechanism for transferring copyrighted files without exposing their illegal conduct to the university network systems or to the "light" of the outside world. The strategy to address this usage is to understand that detecting and stopping all darknet traffic is not the primary goal. The goal is to change the students' behavior. Therefore even statistical detection, perhaps by periodically deploying systems around the campus network, like a radar speed detection trailer that is moved from neighborhood to neighborhood, can be an effective means to influence students' behavior.

Can technology solve the problem of piracy of copyrighted works in every instance? Can technology clear all university and college campuses of illegal peer-to-peer filesharing? Technology will never be the entire solution. Technology is just one of the essential tools to combat piracy on campuses, and as the title of this hearing indicates, technology CAN reduce the number of violations and play a major role in supporting universities' and colleges' efforts to address this most important issue.

Thank you for the opportunity to appear before you today and I will be happy to answer any questions you may have.

BIOGRAPHY FOR VANCE IKEZOYE

Vance Ikezoye co-founded Audible Magic in 1999. He has over twenty years of experience in high technology sales, marketing, and technical support including thirteen years at Hewlett-Packard Company. At HP he was involved in both the computer systems and medical products businesses. After HP, Ikezoye joined Trade Reporting and Data Exchange Incorporated, a VC-funded information company startup, where he served for five years in the positions of Vice President of Sales, Marketing, International, and Business Development. During that time, he developed distribution channels in the U.S., Europe, South America, and Asia. Ikezoye holds a Bachelor's degree in Engineering from U.C. Berkeley and an MBA from the University of Pennsylvania, Wharton School.

Chairman GORDON. Thank you, and Dean Elzy, you are recognized for five minutes.

STATEMENT OF MS. CHERYL ASPER ELZY, DEAN OF UNIVERSITY LIBRARIES AND FEDERAL COPYRIGHT AGENT, ILLINOIS STATE UNIVERSITY

Ms. ELZY. Chairman Gordon, Congressman Hall, and Members of the Committee, thank you for the opportunity today to share with you about Illinois State University's Digital Citizen Project.

Illinois State University is a typical university campus of 20,000 students, great faculty, and great kids. They are not inherently bad people. They are like college students everywhere, sharing movies,

music, TV shows, games, and software, a good deal of it without copyright permission. Our campus is no different.

I described the Digital Citizen Project in detail in my first Congressional testimony before the House Subcommittee on 21st Century Competitiveness last fall, but briefly, this project started back in 2005, when we received nearly 500 copyright violation notices. The pivotal moment for me came personally, though, when we received four subpoenas for students who were going to be sued. I think I felt the situation more deeply because I, myself, have a son at Illinois State. What would I think or how would I react if this was my child being sued? To tell the truth, I would be raising hell with the university for not protecting my son. Why did they let him do this? Why wasn't someone watching?

But what could ISU do? The simple answer seemed to be why don't we go ask them what they want, them in this case was the RIAA. So we did. Though no institution had actually come to them before, the good news is they were willing to talk, and that 28 months ago marked the beginning of our project.

From the first the project leaders felt it was crucial to work with everyone, literally everyone in solving this issue. We have worked closely with RIAA and MPAA as our main long-term project advisors and supporters. We are also partnering with EDUCAUSE and the American Council on Education, and we have talked to the American Library Association and the Association of Public Television Stations. From the monitoring and enforcement industry we have had Packeteer on campus for a long time, and we have talked to or worked directly with Audible Magic, Red Lambda, enterasys, E–Telemetry, Allot, SafeMedia, and others. We are investigating still more like the Bradford Networks. Legal digital media services we have met with include Cdigix, Ruckus, Apple, Napster, Pass Along, and XM Satellite Radio. New ones surface almost every day. We came to Capitol Hill on five occasions and met with the staffs of dozens of Congressmen, Senators, and committees, both Democratic and Republican. We have gone to almost a dozen agencies looking for funding, and we are still looking. We have even talked at some length with the Electronic Freedom Foundation. They gave us what we considered high praise when they said, after a long conference call, that our project sounded "as good as they could hope for."

Digital Citizen is designed to incorporate education, monitoring, legal digital media services, fair use and easier copyright permissions, K–12 education and ethics training and rewards for good digital citizenship. Overall, the long-term goal of the project is to provide a consumer-reports-like study, if you will, on the services and systems that are out there or just coming on the scene so higher ed will be able to make informed, fiscally-responsible decisions.

As to funding, well, funding is hard to find. We were fortunate to receive grants from several entertainment companies and associations, but new and different approaches like ours to rapidly-evolving challenges like campus piracy, don't fit neatly into existing grant categories. It is also hard to find funding because many find it easier to talk about the symptom, downloading, than to fix the root problem, which is changing behaviors and culture.

Our project timelines were originally based on a three-year project; however, it has taken us two years to get sufficient funding to get started. We have only now begun to get to the heart of the research and analysis. Technically, our project has been funded for 18 months, and the clock began five months ago. Without new dollars the project will end July 1 next year. Our early research and data so far confirmed many expected outcomes and revealed some surprises. Please ask me about those later if you would like to know more.

If decision-makers from other campuses came to us today, and they have already started, to find out what to do, we wouldn't have an answer. It is too early. The monitoring technologies don't seem to be fully ready to do what Congress or the entertainment industry wants yet. A consumer study is desperately needed so side-by-side comparisons, benefits, and features can be determined. Both monitoring systems and legal digital media services need to be evaluated, and this all needs to happen now. A consumer study can help the entertainment industry as well by providing reliable, tested feedback. But technology is not the answer. The 911 Commission Report says that "Americans' love affair with technology leads them to also regard it as the solution, but technology produces its best results when an organization has the doctrine, structure, and incentives to exploit it."

Doctrines, structure, and incentives. That is what ISU has put together in the Digital Citizen Project. Your help is essential in directing the conversations toward improvements and testing of emerging technologies, and support for the comprehensive efforts of the Digital Citizen Project and other comprehensive programs like ours, that will be invaluable.

Thank you.

[The prepared statement of Ms. Asper Elzy follows:]

PREPARED STATEMENT OF CHERYL ASPER ELZY

Chairman Gordon, Congressman Hall, and Members of the Committee:

Good afternoon. I am Cheryl Elzy, Illinois State University's Dean of University Libraries and our designated agent for notification of claims of infringement under Section 512(c) of the *Digital Millennium Copyright Act* (DMCA). In other words, I am the DMCA agent on campus. Thank you for the invitation to appear today to share with you Illinois State University's plans to address peer-to-peer downloading on our campus. The overall project has come to be known as the Digital Citizen Project. In the hearing today I will share with you ISU's story of how this program came to be, what we've learned, and where we're going.

But first, I'd like to thank the Committee for its word choices in titling this hearing. *"Reducing"* violations is realistically probably as much as any of us can hope for whether it's from an industry perspective or a technology view or a cultural bias—at least at this time. While this is a hearing before the Science and Technology Committee, with all respect—technology is only a means to an end in a whole lot of ways. Illegal peer-to-peer downloading is NOT solely a technology problem. It doesn't have a "technology" solution alone. The discussion should be about legal access to materials and other information resources. We should be talking about connecting users with the right tools. An added focus has to be on education and changing behaviors. How we do that is what the Digital Citizen Project has been exploring for the past twenty eight months and will describe for you today.

ILLINOIS STATE UNIVERSITY AS AN INSTITUTION

By way of background, Illinois State University is an institution of about 20,000 students with nearly 18,000 of those being undergraduates. The first public university in Illinois, Illinois State University was founded in 1857 as a teacher education institution, a tradition still very much in evidence today as Illinois State is among

the top five producers of classrooms teachers in the Nation and has more alumni teaching in classrooms today than any other university in the country. Our institution is a comprehensive University offering more than 160 major/minor options in six colleges delivered by around 700 outstanding faculty. Students benefit from "the small-school feeling they get from this large university, and the incredible opportunities they encounter." (Yale Daily News Insider's Guide to Colleges, 2000)

We are a typical campus: great students, great faculty, never enough money or space or time. Like every other campus across the country, our students, our faculty and staff are not inherently bad people. They don't carry off armloads of CDs from the local music store. They aren't ripping through Blockbuster with dozens of movies under their jackets. But studies continue to show that college students everywhere share music, a good deal of it without copyright permission. Add to that movies, videos, and television programs. And games. And software. Our campus is no different.

Technology today makes sharing movies and music easy. Everybody's friends and colleagues download, or so users believe. They think it's not hurting anyone really. It's anonymous, quick, direct, and easy. There is no one easy solution, no shrink-wrap fix that will make the students stop or make this problem or the DMCA complaints go away. We at ISU believe the solution to this overwhelming and all-pervasive problem lies in education coupled with enforcement of existing laws and direct avenues to legal ways of getting the tunes, the tracks, the games, and the movies that are an integral part of today's student and faculty lives.

The scope of the problem is national. It's worldwide. It's not just higher education. It's junior high and high schools. Sometimes even grade school, as early as third grade according to what we've finding. My purpose here today is not to talk about the global landscape or the national picture. I'm here to share what one typical university with typical students is trying to do to address not just the symptom of the problem—the illegal downloading of digital media, but its comprehensive root cause.

THE HISTORY OF THE DIGITAL CITIZEN PROJECT

I described the history, background, and varied parts of the Digital Citizen Project in extensive detail in my first Congressional Testimony before the House Education and Workforce Committee's Subcommittee on 21st Century Competitiveness in a hearing entitled *"The Internet and the College Campus: How the Entertainment Industry and Higher Education are Working to Combat Illegal Piracy" on September 26, 2006. (http://republicans.edlabor.house.gov/archive/hearings/ 109th/21st/piracy092606/elzy.htm)* I would be honored and pleased if you would check that testimony if you need more information than is presented here.

To describe the project briefly, though—during the winter of 2005 we at ISU became progressively more dismayed as the number of copyright complaints began increasing dramatically. In 2001, 2002, and 2003 we received a few scattered complaints throughout the year, but nothing particularly overwhelming. By 2004 Illinois State was seeing a little more DMCA activity, but in 2005 everything just seemed to explode across our screens. Sometimes there were days when we were getting 20 or 30 notices a day, several days a week, primarily from entertainment industry associations. In the fiscal year ending in June 2005, Illinois State University had received 477 formal DMCA complaints from the Business Software Alliance, the Entertainment Software Association, Sony, Fox, NBC, HBO, MPAA, and RIAA. The problems on campus were stemming from activity in the residence halls, Greek houses, other places on campus, and dial-up access. Staff time to manage these increased exponentially. Our student judicial office saw much heavier traffic referred to them for discipline. Follow-ups and tracking seemed to take forever.

Naturally we began asking questions among those working in the appropriate use areas on campus. Why the sudden rise in numbers? Were our students doing more illegal downloading or were they just getting caught? Were we somehow targets of new enforcement campaigns? Why the rise at universities when the problem is so much more widespread? What was all this costing us? How much costly technological bandwidth was this taking besides the obvious investment in staff? How could we possibly be satisfied with simply reacting, instead of being proactive on the part of our students?

The pivotal moment for me personally came when we received four subpoenas for information on some of our Illinois State University students who were going to be sued in federal courts for copyright infringements. At that moment my campus was faced with decisions with no options particularly attractive. Do we comply (as other campuses had) or do we fight release of the information (as still other campuses had)? Do we warn the students about the subpoenas or do we stand aside? I think I felt this whole situation more deeply because I myself have a son attending Illinois State. What would I think or how would I react if this was my child? The truth

is I'd be raising hell with the University for not protecting my son! Why did they let him do this? Why did they make it possible for him to get into this mess? Why didn't they block this kind of thing? Why wasn't someone watching?

The university complied with the subpoenas and provided the information. Then we stepped back to think and to plan. What could we do to protect our students while still complying with the law? How could we educate and direct our students? What could we do to police ourselves? The rather simple solution seemed to be, literally and in the exact words I used back in February two years ago, "Why don't we go ask them what they want us to do?" "Them" in this case was the Recording Industry Association of America. So we did. Though no one, no institution had actually come to them before, the good news is that they were willing to talk. And that, 28 months ago, marked the beginning of our Digital Citizen Project.

One of our first steps was to find out what other institutions were doing to combat illegal downloading and reduce DMCA complaints through scholarly literature, through conferences, through the press. Today, over two years later, more and more colleges and universities are taking significant steps to tackle the illegal downloading issues. But judging by what we could find in the professional literature 28 months ago, the answer then appeared to be: not much. We knew anecdotally that some institutions were actually throwing the complaints away. A number of institutions were delivering educational or public service campaigns, often with a unique local twist. There were a few that were putting up a legal music or movie service or two and hoping students, in particular, would be attracted to the legal approach. A few other universities simply shut down all bandwidth available for peer-to-peer activities of any kind, legal or not. Some reported limiting the amount of bandwidth available to peer-to-peer applications. All of these programs reported little or varying degrees of success. From our perspective, most universities and colleges seemed to be waiting for someone to prove to them that the problem was real and needed attention. Others were waiting for "the" solution.

THE PROJECT DESIGN

Rather than confronting campus piracy with a single approach, we worked with RIAA and ultimately MPAA to develop a multi-faceted approach to combating piracy on campus. Early on the discussions focused on three things—monitoring and enforcement, legal services, and education—but subtle changes began to emerge very quickly. The first was to move education to lead the list. That was significant to us as educators. A critically important aspect for me as a librarian was a crystal clear definition of fair use of media in the classroom along with easier paths for copyright clearance of media we needed to use. Another addition to the program focused on K–12 education and ethics. It is widely accepted that downloading behaviors start much earlier than when a student arrives on a college campus—and in fact student behaviors are learned in high school or before, at home from their parents, at school, and at play. Finally, to attract students to a comprehensive program of legal, ethical online behavior we wanted to offer some sort of rewards for good digital citizenship.

Overall, the long-term goal of ISU's Digital Citizen Project is to create a nationally recognized program that could be cost-effective, that is based on comparison and research of the products currently available, and that is replicable on other college campuses. We are far from there, but we're laying a solid foundation. And we absolutely know that there is no one-size-fits-all institutional solution. Nor is there a one-size-fits-all technology solution. Not at all. But if a central place for education, conversation, trial, and admittedly error can get a foothold, then all of higher education benefits. We would like to be that central place to serve as a resource for higher education, a bridge between education and the entertainment community, a funnel for positive feedback and advice to vendors, and a repository for educational materials on cyber-ethics, legal downloading, and system or software implementation. We want to provide a "consumer report-like" study, if you will, on the services and systems that are out there and just coming on the scene so higher ed will be able to make informed, fiscally responsible decisions on what to do on each of the 4,000 campuses across the country.

THE PROJECT PARTICIPANTS AND CONTACTS

From the first days of this project 28 months ago the project leaders felt it was crucial to work with everyone—literally everyone—in solving this issue. We contacted associations. We talked to vendors. We went to conferences to make other contacts. We came to Capital Hill in search of support. We have talked with or partnered with RIAA and MPAA as our main long-term project advisors and supporters. We are also working closely with EDUCAUSE and the American Council on Education, and we have talked with the American Library Association and the

Association for Public Television Stations. From the monitoring and enforcement industry we've had Packeteer on campus for a long time, and we have talked to or worked with Audible Magic, Red Lambda, enterasys, e-Telemetry, Allot, SafeMedia, and others. We've investigated still more, like Branford Networks. Legal digital media services we've met with include Cdigix, Ruckus, Apple, Napster, Pass Along, and XM Satellite Radio. New ones surface almost every day. We came to Capital Hill on five occasions and met with the staffs of dozens of Congressmen, Senators, and committees both Democratic and Republican. We've gone to almost a dozen agencies looking for funding, and are still looking. We've even talked at some length with the Electronic Freedom Foundation (EFF). They gave us what we considered high praise when they said, after a long conference call, that our project sounded "as good as [they] could hope for."

DIGITAL CITIZEN PROJECT FUNDING

As to funding—the biggest financial supporter of this project to date is Illinois State University itself. The University has contributed staff time for a wide range of people working on the Digital Citizen Project from CIOs to network engineers to researchers and staff, salaries, space, equipment, supplies, and more with an estimated value of over $450,000. Beyond that we've gotten formal research grants from the University, federal funds in the form of a $68,000 Library Services and Technology Act (LSTA) grant through the Illinois State Library, and substantial support through the entertainment industry. Specifically, funding has come to the project from Viacom, Time/Warner, NBC/Universal, a research conglomerate called MovieLabs, RIAA, and MPAA. We are aggressively seeking public or higher ed funding to balance the support base of the project to avoid even the appearance of being a "bought-and-paid-for study." The data we produce and the findings we share must be real and must be defensible academically. We must remain balanced, unbiased, and neutral in order to work productively with all the project partners—some of whom hate each other, and some of whom are suing each other. Funding is hard to find because new and different approaches—like ours—to rapidly emerging and changing challenges—like campus piracy—don't fit neatly into existing grant categories. It's also hard to find funding because most find it easier to talk about the symptoms (downloading) than to fix the root problems—changing behaviors and culture while adapting different business and marketing models. In a nutshell, we need more funding and we need more time.

THE PROJECT TIMELINE

Regarding time, our project timelines were originally based on a three-year project. However, it's taken us two years to get started. We've only now begun to get to the heart of the research and analysis. Technically and specifically, our project was supported under our current research agreement, for 18 months. The clock began five months ago. Without new dollars, the project will end July 1, 2008. To date, the Digital Citizen Project has captured network data using Audible Magic's technology in August 2005, August 2006, and April 2007. Last summer, we surveyed high school seniors coming to Illinois State about their downloading habits and preferences, and we're doing that again starting the week of June 4. We have completed and have reports on a number of focus groups organized and analyzed by professors on our marketing faculty. We've just completed an extensive, in-depth survey of campus faculty, staff, and students on their attitudes toward downloading—and we're planning two more studies in the fall. Perhaps most interesting—we're journaling the problems, issues, and surprises surrounding the implementation of the project, the systems, and the research. And if anything highlights the changing landscape of this project, it is our experiences. For example—one firm changed its business model five times in the last 28 months, moving from charging our campus $40,000 for its service to being free and directly marketed to students. Another leader went out of the downloading business all together. A supplier of monitoring systems wanted us to change how we register our students on the network rather than adapting to the existing environment. We discovered in working with another vendor that to get the data we wanted with one company's network monitoring system, required not a single box but multiple ones—multiplying the projected expense beyond what any campus could afford. One system initially needed another to work, so a campus would have to buy two systems—not one—to be effective. Misunderstandings on conference calls and e-mails occurred regularly. A classic misunderstanding occurred when one vendor told us we needed to install their "secret kernel" on our network. Our engineers freaked! We weren't going to put anything on our live production network that we didn't fully understand, let alone something SECRET!! As we learned later in probably the 10th conference call—the vendor wanted us to load their cGrid kernel, their software! But that

shows the mistrust, the misunderstandings, and the huge amount of time it takes to resolve even simple issues in this project. These examples may seem silly or incidental to you—but they all take time, explanation, resources—and they impact what we should expect to tell our colleagues about ease of implementation or our vendor partners about what they might want to change.

THE PROJECT'S FUTURE

What we expect to do over the next thirteen months covers a huge spectrum of activities. We are testing the data gathering capabilities of network monitoring right now in anticipation of a major, in-depth, comprehensive study in September. We are, at this moment, conducting very detailed interviews with student downloaders to get a better understanding of what they do and why so we can design educational programs that might have an impact on campus piracy. We'll be conducting two more behavioral research studies in the fall, designing what we are calling "birdtrax" (named for our mascot Reggie Redbird), which will outline the options for legal digital media services, sorting out a financial plan to recover some costs long term, and implementing some public relations options. We'll pilot and launch an escalated response monitoring and enforcement system in late fall. "birdtrax" will become a live site that students can use to learn about and navigate to legal digital media services. As varying layers of enforcement are employed, impact on downloading traffic will be studied. All through the next thirteen months in order to continue the study, the project leaders will be writing grants and seeking funds to extend and expand the project capacity.

As stated above, the Digital Citizen Project's long-range goal is that we will serve as a kind of "consumer's reports" on the digital media scene, testing, reviewing, and implementing new services as they emerge in the market while serving as a resource to higher education on the education side of this equation. We absolutely know that we very well may provide evidence of what DOES NOT work as much as what does. Illegal downloading may need far more effort and much broader approaches than we can bring to bear on the problem as a single institution.

Working with vendors to secure participation in our "consumer's report" approach to the downloading issues has had its challenges and successes. An advantage we have that also becomes a concern is that we are doing our research on a live network. It's an advantage because it provides real-world evidence. It's a concern because any missteps can bring our campus network down. So we are now developing a proposal that will fund a test network so we can work with some of the softwares and systems outside of our live production network. We're also working on a plan that will compartmentalize various systems on the live network—such as using different dorm complexes to analyze the effectiveness of different systems at the same time. Another challenge in the consumer report-like model is convincing most of the vendors that they won't be the ONLY service or software at Illinois State University. However, testing as many systems and services as we can is something we must do for the comprehensiveness and integrity of the Digital Citizen Project and its research goals. At one extreme—notably with our fellow witness, Audible Magic—our project and our expertise has been so valued that we are working in complete partnership to develop new modules and releases of that company's product. At the other end of the spectrum, we have been completely ignored in our repeated attempts to bring one of the leaders in the downloading field into our project. Some vendors who really want to be a part of ISU's Digital Citizen Project and birdtrax just aren't ready for complete implementation and roll-out yet, so we hope to include those in the next phase of the research and offerings. Your assistance in urging vendors to participate in our study for the benefit of higher education is as important as urging higher ed to do something about campus piracy. Higher education needs this kind of comparative information.

RESULTS OF THE DIGITAL CITIZEN PROJECT SO FAR

Downloading is a complex issue. Universities are complex operations. Testing and implementing new technologies is an extraordinary undertaking. Research is a complex task. There are privacy issues, financial issues, legal issues, practical issues on a live network, and cultural issues. But to be effective, the Digital Citizen Project must be comprehensive. So the entire spectrum of what we're looking becomes exponentially complex.

However, we do have some early results to share.

Illinois State did begin limiting peer-to-peer traffic very early—back in 1998 as Napster and other downloading services began to take off. We use Packeteer to shape the bandwidth on our campus so that not more than five percent of our capacity can be used for any kind of peer-to-peer application. It's important to stop here and state our project's strong opinion that a campus cannot unilaterally block all

peer-to-peer. There are too many legitimate uses of P2P—cooperative research file transfers, software upgrades, library digital files, distance education requirements, and more. By shaping our bandwidth and implementing a more selective monitoring system, we believe we can meet two needs—supporting legitimate peer-to-peer uses while blocking the sharing of copyright media.

- Our work with the technology available so far has shown us several things already, and one of the most important is understanding how network tools and appliances work within our network The twists, and turns, and varying demands of each system make getting real, accurate, comprehensive data on real peer-to-peer traffic extremely difficult. There are problems with encryption of illegal files. Some files are sent over different parts of our network, making them more difficult to capture. The volume of data we have to analyze from our network overall is staggering, even in just one month's capture. Very preliminary results showed that Audible Magic captured 23 million files of all kinds—legal, illegal, encrypted, and more—on our network in April 2007 alone. The amount of recognizable P2P—even with all the recognition problems—is sizable, though probably not at all out of line with activity on other campuses. In only the first five days of the month individuals downloaded copyrighted files ranging from one file to 466 signatured files.
- Most problematic for the monitoring technologies overall, though is the lack of identifiable tags or electronic signatures on digital files. While the percent of signatured—and therefore, findable—unique titles has grown over the last two years from 11 percent to 51 percent, there is much more to be done. Signatured titles right now are almost exclusively music files. Virtually no movies have the electronic signature. To find movies takes elaborate analysis and actually LOOKING at the tags, descriptors, or metadata. We can't stop what we can't find. We are working with the industry to devise an electronically, automatically recognizable system of coding files. The monitoring systems will be more effective and comprehensive.
- We're finding that our students are well-versed in prime sites for downloading copyright material. 46 percent use BitTorrent, followed by Gnutella, Limewire, and Morpheus. Darknets—or sharing files within the campus network—account for about 16 percent of the traffic we can identify in the network snapshots we've done. Industry sources pegged this at 45 percent while our own network engineers estimated maybe five percent. The actual data proved that both ends were off a bit.
- In our early snapshots we found not as many computers on our network use peer-to-peer applications. Of the 13,000 computers on our network, only 26 percent used peer-to-peer services, legal or illegal. That is a little less than 3,400 machines, a figure that is lower than any of us had expected. Apparently the anecdotal evidence of "everybody's doing it" may be off base. But of the 3,400 computers using peer-to-peer, 97 percent of the traffic originated in the residence halls, indicating that we may be able to concentrate our educational efforts on those groups.

In addition to what we've found out about the technology and what it can do, we've learned more about our students and their behaviors.

- We surveyed high school seniors who were coming to campus to register for classes at ISU last summer. Notice, please, I'm not calling them college freshmen, but rather high school seniors. Their attitudes and behaviors had been established before any exposure to our campus. We probed their use of digital media and what kind of mobile players they used. Of the 217 responding students, 89 percent reported they had a portable music player. 67 percent of those devices are Apple iPods with the rest scattered among 26 different kinds of players. 93 percent played music and 51 percent watched movies/TV/videos from their computers. When asked how these incoming students acquired their music and movies, the responses demonstrated an extreme range of sources from actually buying CDs to commercial services like iTunes. Various P2P networks such as Limewire, Bearshare, and BitTorrent were mentioned by 39 percent of the seniors. While not testing the legal vs. illegal use of these networks, the naiveté we've seen elsewhere shown through as we found comments such as "Not legally," "pirate from XXXX" or "illegally downloaded." To us, this absolutely shows that our new students come with habits entrenched in a digital lifestyle.
- In our surveys and focus groups this spring, we learned that many students started downloading in sixth grade, or when they are about 10–13. 55 percent

in the focus group study downloaded often, averaging 23 songs per day. They believe downloading saves them time and money, but that they would use legal alternatives if they were easy to use, had the kind of media in their digital libraries that the students wanted, and they were free. When asked, though, if the students could name any legal digital media services, they could not. In fact, many seemed to assume that iTunes might be illegal when it is not. Most aren't going to quit until there is some deterrent.

More on these studies will be published in the coming months in the academic literature.

One of the most important things we feel we've learned in the course of the last 28 months is that no monitoring or blocking system will completely eliminate DMCA complaints. As we said, learning what DOESN'T work in our project may be as important as what does—particularly on this point. Nothing appears to be effective enough to stop all copyright violation notices at this point. We're getting there, but not yet. And while no system has to be 100 percent effective before it is implemented, it is premature to ask all college campuses to invest tens of thousands of dollars in systems that aren't ready yet. We've all heard from other hearings that "the hammer is coming." But if the hammer drives nails that break or bend, the construction project is ineffective. Leaks will occur. And certainly, if Congress asks all 4,000 colleges and universities across the country to implement monitoring systems over a very short period of time—from our experiences it would seem impossible for vendors to supply our needs, let alone the tech support we all will absolutely have to have to make the systems operational. We've been working with one industry-leading vendor for 16 months to try to bring them to campus for a test—and we're still not there.

CONCLUSIONS

If campus decision makers came to the Digital Citizen Project today—and they've already started—to find out what to do, we wouldn't have an answer for them. It's too early. The monitoring technologies don't seem to be fully ready to do what Congress or the entertainment industry wants. Yet. Yes, they may REDUCE campus piracy. From our early experiences and data, we believe the technologies do not yet do what higher education wants—to STOP the DMCA complaints completely.

The other technological equation is legal digital media services. iTunes is not the only answer. 30–40 percent of the students have some other sort of player not compatible with iTunes. Legal services need to market their services more effectively so student can at least name one. They need to listen to their customers and be comprehensive, easy, and—of course you would expect this—free. Studios have to help them by supporting digital distribution systems. Movie studios need to get in the game because we're suspecting from early findings on our campus that far more bandwidth is used in downloading movies, videos, TV shows than songs. Video may be just as pervasive a problem as music. Right now it's far harder to track.

Higher education needs more information. A consumer study like we're proposing is desperately needed so side-by-side comparisons, benefits, and features can be determined. Both monitoring systems and legal digital media services need to be evaluated. And this all needs to happen now.

The consumer study can help the entertainment industry as well by providing feedback, gaps, strengths, needs, and more. Audible Magic, an early and strong partner in our Digital Citizen Project, was very open to taking our feedback and both modifying their product for our network environment, but also adding new functionality. They ran with our wishes to develop a new product in conjunction with our ISU programmers that we believe will be very useful to other campuses. This is an example of the kind of partnership that should be promoted and rewarded.

But again—technology is not THE answer. The 9/11 Commission Report says that "Americans' love affairs with [technology] leads them to also regard it as the solution. But technology produces its best results when an organization has the doctrine, structure, and incentives to exploit it." *(http://www.911commission.gov/report/911Report_Ch3.htm)* What is needed is "the doctrine, structure, and incentives"—a comprehensive program of education and ethics on campus and in the schools, cultural change, enforcement, high quality legal avenues for entertainment, and some sort of positive reinforcement for good digital citizenship. That's what we believe must be developed and tested for effectiveness. Think of seat belts. In 1963 Congress passed its first seatbelt law—44 years ago. In 2006, seat belt usage was determined to be 81 percent (*http://www-nrd.nhtsa.dot.gov/nrd-30/NCSA/RNotes/2007/810690.pdf*). We've worked over 40 years to get people to change a behavior that will save lives, and we're still at only 81 percent compliance. How long will it take to change the behavior, the ingrained culture of illegally downloading copy-

righted materials? Early education and great technologies hold the key. We have proven at Illinois State that we can be effective in researching the problem. We are certainly successful in being able to work with everyone—higher ed, industry, vendors, associations, Congress, and more. We need funding and time to create a true test environment and a living laboratory on our campus to work with the technologies and track what works and what does not.

Your help is essential in directing the conversations toward improvements in and testing of new technologies. Your assistance is critical in directing all of us to focus on education starting with the Nation's very young, and your involvement in a national conversation on practical fair use and copyright permissions, can point the way to creating great role models. Your support for comprehensive efforts like our Digital Citizen Project, with funding and by utilizing us as a knowledgeable resource for Congress and higher education in general, will be invaluable.

For more information visit *www.digitalcitizen.ilstu.edu*

BIOGRAPHY FOR CHERYL ASPER ELZY

Cheryl Asper Elzy currently serves as Dean of University Libraries and as the campus federal DMCA copyright agent at Illinois State University in Normal, Illinois, where she manages the operations, services, collections, and programs of the 1.6 million-volume Milner Library. She came to Illinois State in 1981 to teach in the library science program after serving on the faculty of Quincy College as Assistant Director of its library. Dean Elzy also served as director of the Chenoa Public Library and Gridley Public Library in the 1980's as part of a unique shared staffing program funded by the Illinois State Library in Springfield to bring professional librarians to small libraries.

Dean Elzy joined Milner Library's faculty in 1984 where she has held a number of increasingly responsible positions including head of the Education/Psychology/Teaching Materials Center Division, Associate University Librarian for Personnel, and Associate Dean of University Libraries. Professor Elzy was named Interim Dean of University Libraries in 1996, and Dean in 1998. She is active in the American Library Association, the Library Administration and Management Association, the Illinois Library Association, and the Council of Directors of State University Libraries in Illinois.

Dean Elzy earned three degrees at the University of Illinois at Urbana/Champaign, including two advanced degrees from the Graduate School of Library and Information Science. She has published in the fields of reference services evaluation, evaluation of collections, end-user studies of reference databases, and in children's literature research. More recently Dean Elzy's research has focused on issues surrounding the illegal downloading of copyrighted songs, movies, videos, and games on college campuses.

Chairman GORDON. Can't beat them out if we are not getting action. Good job and thank you, and now Dr. Jackson, you are recognized for five minutes.

STATEMENT OF DR. GREGORY A. JACKSON, VICE PRESIDENT AND CHIEF INFORMATION OFFICER, UNIVERSITY OF CHICAGO

Dr. JACKSON. Mr. Chairman, Mr. Hall, Members of the Committee, I am Greg Jackson. I am the Vice President and Chief Information Officer at the University of Chicago. Thank you for inviting me here today.

Let me summarize five points from my written testimony. First, the university's business centers on intellectual property. We patent, copyright, publish, and teach. Protecting our rights to all this is important, but so is access. Research and teaching depend on the convenient availability of intellectual property. We need to work together across organizational and political lines to find the elusive right balance between mechanisms that protect intellectual property and mechanisms that make it accessible. Staking out irreconcilable adversarial positions won't achieve that.

Second, the university deplores violations of copyright law. We received 57 DMCA complaints last year and expect about twice that many this year. We handle these aggressively by immediately disconnecting the offender. Before restoring connections, we require first offenders to meet with the Dean on the record to emphasize the seriousness of the offense. We fine second offenders 1,000 bucks. In addition, we paper the campus with posters like these. We discuss the issue at orientation and in class, and our acceptable use policy covers it. Periodically I remind the entire community by E-mail that the university takes copyright offenses seriously and that they can have very negative consequences.

Our approach has yielded good results. DMCA complaints involve less than half of one percent of our community. Over five years we have had only six repeat offenders.

Third, the principle drivers of infringement are business related. Movie and music producers serve their online customers inconsistently, incompatibly, inefficiently, inconveniently, and incompletely. Music purchased legally from Microsoft, for example, can't be used on Apple devices or vice versa. Pricing seems high and managing keys and licenses is a major hassle. Most movies remain unavailable, and no one offers Beatles tracks. If the right thing keeps falling short of customers' reasonable expectations, too many customers will keep choosing the wrong thing.

Fourth, network-based anti-infringement technologies fail within high-performance networks. As I detail in my written testimony, the Internet transports not distinct, intact files but rather files chopped up into packets and then shuffled together. Only limited address and type information and not content is readily available in transit. Address and type alone cannot accurately identify illegal transfers and reconstituting file content for blocking at network speeds can be a daunting challenge. This is why the dominant anti-infringement technologies fail within high-performance networks; both traffic-shaping products, such as Packeteer, Red Lambda, and Clouseau; and signature-matching products such as Audible Magic. These may work today at the relatively slow borders between campuses or dormitories and the regular Internet as we have heard today, but they will fail even there as strong encryption becomes commonplace and legitimate applications of peer-to-peer filesharing expand.

Moreover, as Apple, Amazon, and others sell unprotected copyrighted music and movies, legal network transmissions will become identical to illegal ones, further hampering anti-infringement technology.

Finally, technological obstacles to behavior have limited counter-productive effects. We have learned this lesson from long experience with intensively-networked university communities. The only successful, robust way to address problems that involve personal responsibility and behavior is with social rather than technical tools. We must teach and persuade people that certain behaviors are socially and economically counter-productive for their own communities. If owners, publishers, transmitters, and users do that teaching together, collective benefit will trump individual malfeasance. If we instead try to restrict behavior technologically, the

only result as Dr. Sannier said earlier, will be an arms race that no one wins.

I hope that the Committee translates this lesson into effective policy and collaborative practice, and I appreciate the opportunity to provide whatever help I can.

[The prepared statement of Dr. Jackson follows:]

PREPARED STATEMENT OF GREGORY A. JACKSON

Mr. Chairman, Representatives of the great State of Illinois, and Members of the Committee, I am pleased to be here today. My name is Greg Jackson. I am Vice President and Chief Information Officer at the University of Chicago, where I have overseen central information technology and services for almost eleven years. Before that I was MIT's Director of Academic Computing, and before that a statistician and faculty member at Harvard and Stanford.

Two high-level policy questions frame our discussion today. The first is whether the copyright law that has grown up around industrially-organized publishing remains relevant and productive in today's widely distributed information economy. The second is to what degree network service providers should be responsible for illegal use of their networks.

I know that the Committee has engaged these larger questions in other hearings. Since I can claim no special expertise with regard to the larger questions, I will concentrate on the two topics I have been asked to address based on my experience at the University of Chicago: how we handle DMCA and related incidents, and the feasibility, in research universities like ours, of technologies one might use to reduce the illegal sharing of copyrighted materials.

My testimony emphasizes five key points:

- The University's business centers on intellectual property;
- Like most of its peers, the University deplores violations of copyright law;
- Market shortcomings are the principal drivers of infringement;
- Network-based anti-infringement technologies fail within high-performance networks, and eventually they will fail more generally; and
- Technological obstacles to behavior have only limited and transitory effects.

Let me begin with a few words about the University. We are a large private institution, one of the world's major research universities. We operate one of Chicago's principal medical centers and, through subsidiaries, two DOE research laboratories, Argonne and Fermi. We have a $2 billion operating budget, 13,000 students, 2,000 faculty, 5,000 staff, 150 buildings in five states and four foreign countries, 25,000 telephones, and—most important for today's topic—a high-performance network using about 2,500 switches and routers to connect our 25,000 digital devices to each other, to research universities and labs worldwide, and to the Internet.

1. The University's business centers on intellectual property

Our research produces not only deeper understanding of how the world works, but also concrete products including many inventions and creative works. Our teaching instills in our students not only concrete knowledge and skills, but also insights into what's worth doing and what isn't, what's right and what's wrong. We protect our intellectual property: we patent inventions, copyright works, distribute online journals, value distinctive teaching, and so on. Yet research and teaching, the heart of higher education, also depend on access to intellectual property. This has implications for course materials, for our libraries, for publications, for the University of Chicago Press, for our relationships with outside entities, and in many other domains.

It is important to us that patents and copyrights be enforceable—even though in many cases we license our intellectual property, and especially our research, for free. But it is also important that we be able to do the best possible research and teaching, that technology advance rather than degrade our ability to do that, and therefore that technology promote rather than deter access to intellectual property.

A key challenge for all of us—copyright owners, publishers, transmitters, enforcers, and users alike—is to find the elusive right balance between mechanisms to protect intellectual property and mechanisms to make it accessible. Tradeoffs are inevitable. We should all be working together, across organizational and political lines, to find reasonable, manageable compromises among our diverse needs, rather than unilaterally and adversarially staking out fundamentally irreconcilable positions.

2. Like most of its peers, the University deplores violations of copyright law

The University of Chicago received 57 *Digital Millennium Copyright Act* (DMCA) complaints in 2006. At the current pace (33 complaints through April 30), we will receive about 130 complaints in 2007. Those complaints involve only about one half of one percent of our community. 58 percent of last year's complaints involved music, and most of the rest involved movies, TV shows, or software; this year the music percentage has dropped to 52 percent. (I should note that the MPAA "top 25" listing has an incorrect DMCA count for us—it's about ten times the right number. We have asked MPAA to clarify or correct this, but thus far have received no substantive response.)

The DMCA, as we understand it, requires the University, as a "network service provider," to end violations when we receive a valid, accurate DMCA complaint. (A valid complaint requires that data sufficiently detailed to locate the offending computer, plus various other elements including an affirmation and a signature, be sent to the University's "DMCA agent"—me, in our case.) We deal strongly with DMCA violations. When we receive a complaint, network-security officers first verify that the offending material remains available, or that our network logs confirm the access cited in the complaint (this is what makes a complaint accurate). If the complaint is valid and accurate, network-security officers immediately disable the network connection cited in the complaint, as DMCA requires. In addition, by University policy we identify who was using the connection at the time of the offense, and refer the offender to the appropriate disciplinary process.

For first offenders this means a formal hearing before a Dean (or an HR officer in the case of staff) and a file notation, after which we restore the network connection. (Very few offenders dispute the violation, although many assert—often with good reason—that the offense resulted from negligence rather than intent.) For second offenders we impose a fine of $1,000, the proceeds of which become financial aid for others. Over the past five years we have had just six second offenses.

In addition to the disciplinary process for offenders, we communicate broadly with the community on this topic. We deploy humorous but persuasive posters. We discuss the issue at student orientation. Faculty and instructors discuss it in class at relevant moments. It is covered by our acceptable-use policy. About once a year, I personally remind the entire community by e-mail that the University takes DMCA offenses very seriously and that they can result in very negative consequences.

Many of our DMCA offenses, we believe, result not from intentional distribution of copyrighted material, but rather from how hard it is to disable the public-sharing features of peer-to-peer software. Because of this, we publish a web page providing extensive guidance as to how a user can disable peer-to-peer sharing. Scores of other entities—including RIAA itself—have cited or linked to our materials.

Unfortunately, inaccurate DMCA complaints, discriminatory enforcement, and politically-structured "top 25" lists have proliferated lately. One movie company, for example, has an accuracy rate down around 20 percent, and even though commercial ISPs in some university towns serve precisely the same numbers and types of students who live in campus dormitories, the ISPs receive no DMCA complaints and never make top-25 lists even when the local university does. This is all becoming very problematic, since these problems waste resources, and the inconsistencies and discrimination cause offenders to dispute rather than accept our guidance.

3. Market shortcomings are the principal drivers of infringement

Media producers provide and protect their online wares inconsistently, incompatibly, inefficiently, inconveniently, and incompletely. For example, music purchased legally from Microsoft can't be used on Apple devices or vice versa, pricing seems high, managing keys and licenses is a major hassle, and no one offers Beatles tracks. So long as the right thing remains more daunting, awkward, and unsatisfying than the wrong thing, too many people will do the wrong thing.

Digital rights management (DRM), the principal mechanism vendors use to protect content sold online, involves packaging intellectual property so that it cannot be used without a special digital key. The digital key, in turn, is restricted to a particular customer or device with license to use the content. This is how iTunes, Zune, Ruckus, and Genuine Microsoft Validation work. Customers who want to use content protected by different DRM typically have to use different software—or even different devices—to gain access. Managing keys can be a major hassle, for example when one's device dies or is replaced. Moreover, poorly implemented DRM can disable customers' computers entirely, as one media company unfortunately demonstrated broadly with its CDs not too long ago.

DRM appears to be a good idea. However, it has been plagued by poor execution, and so has come to be a frustrating obstacle rather than a convenient enabler.

Moreover, DRM has become a challenge to security specialists and hackers, who delight in showing how easily it can be subverted. This exemplifies the unwinnable arms race and has induced some vendors to begin selling unprotected content, points to which I will return.

4. Network-based anti-infringement technologies fail within high-performance networks, and eventually they will fail more generally

How Networks Transmit Files

Say that person A wants to send a file to person B. If A and B work at universities, the file might be a pre-publication draft, a three-dimensional x-ray scatter image of a molecule, or the video of a procedure carried out within a containment facility, but the process would be exactly the same if A were sending a personal wedding video or an illegal copy of *Eleanor Rigby* to B. Here's what happens, in simplified form:

1. A's computer chops up the file (which may first be encrypted, for security) into many small chunks, much as I might cut up a large mounted photograph to make a jigsaw puzzle whose pieces would fit in regular envelopes. A "header" on each chunk contains limited information including as the address of B's computer and the kind of data being transmitted—by analogy, think of the addresses and "contains photo—do not bend" notations on an envelope. The encased chunk is now a "packet," in networking jargon.
2. One by one, A's computer sends packets to the network for transmission to B's computer. A's computer sends other files to other places at the same time. The packets from the other files get shuffled with the B-destined file's packets as they leave A's computer.
3. Once the packets reach the network, bucket brigades of routers and switches pass them along—again mixed with others, and again one by one—until each packet reaches its destination. Although packets headed for the same destination usually follow the same path, a great strength of the Internet is that they need not do so. Network equipment constantly monitors flows, and switches to alternate routes when particular paths get clogged.
4. As packets reach B's computer—some from A, some from other sources—B's computer sorts them and requests re-transmission for any missing packets. It then extracts the chunks of data from the packets and reassembles them into the original file.

I highlight four key attributes of this process. First, files move across the network in *discrete packets,* rather than as whole files. Second, packets are *intermingled* with other packets from other files as they leave the source, as they move across the network, and as they arrive at their destinations. Third, packets going from one source to one destination may follow *different paths* across the network. Fourth, this chopping and scattering is *intentionally designed* into the Internet to ensure reliability, speed, and robustness.

As particularly advanced users of networking, colleges and universities typically deploy networks comprising an array of main switches and routers interconnected in a ring or mesh with tentacles reaching out to smaller switches and routers, rather than connect everything to one telephone-like central switching point. Rings and meshes maximize the robustness and efficiency of networks. As a desirable consequence, they also make internal traffic on campus networks especially likely to follow multiple routes between points.

Much as it's easy to attain perfect network security by detaching computers from networks, it's easy to protect intellectual property by locking it in a strongbox where no one can retrieve it, or by disabling networks that might transmit it. The value of intellectual property depends largely on circulation, however, so using a strongbox or disabling networks reduces the value of the property. Implementing the strongbox or complicating the network diverts resources from more productive pursuits. And so the challenge we are discussing today: Can anti-infringement technologies work without degrading the efficiency and productivity of the campus networks critical to research and teaching?

There are two principal network-based technologies for forestalling, detecting, or reducing illegal network filesharing: traffic shaping and signature matching.

Traffic Shaping

Traffic shaping involves handling packets differently depending on information in their headers. Thus, for example, we might assign Web packets higher priority than e-mail, or Berkeley-bound packets higher priority than Emory-bound ones, or lo-

cally-originated packets higher priority than others. Higher priority translates into faster transfers, so varying priorities in this way "shapes" traffic according to policy.

The most common shaping tools are firewalls, which block traffic according to source, destination, or other header attributes. Packeteer, cGrid, Clouseau boxes, or other more sophisticated shapers can also speed or slow traffic according to packet headers. Traffic shaping can be quite effective when offending traffic (a) has stable or predictable header attributes and (b) those header attributes clearly, reliably, and accurately distinguish illegal from legal traffic.

Unfortunately, much illegal filesharing fails these tests. Newer peer-to-peer software routinely switches addresses and ports in increasingly complex ways. It often mixes infringing transmissions with legitimate ones, for example by disguising transmissions as Web traffic or legal transfers. Moreover, a great deal of illegal filesharing no longer uses distinctive peer-to-peer software or protocols. Traffic shaping has thus become rather ineffective against illegal network filesharing, although it remains an important mechanism for network management.

Signature Matching

Signature-matching technologies compare a file's content to a database of abstracted "signatures," and then take specified action when they find a match. The most typical examples are virus or spam checkers, which perform the matching exercise when a computer opens a file or message and block the file if it matches the checker's database. The comparisons necessary for signature matching can be slow, since accuracy requires detailed comparison. However, virus and spam screening appears not to slow things down, mostly because personal computers and e-mail servers operate so much faster than people use files or read e-mail.

Signature matching for network traffic is much more challenging. In order to do high-quality comparison on network traffic, an entire digital file must be available for comparison to the signature database. Accurate signature matching thus entails three requirements: that all packets travel through one network point where they can be gathered and reconstituted, that reconstitution and comparison be as fast as network transmission, and that matching methods and databases identify only illegally transferred files—that is, there can be no false positives. These are the challenges for Audible Magic and similar products.

The requirements for satisfactory signature matching appear unattainable within the typical campus network. (The network border is a separate issue, to which I will return.) First, as I pointed out earlier, a file's packets are mixed in with others, and may travel different routes across the network. This makes gathering and reconstitution en route difficult at best, and often impossible. Second, networks are equipped and optimized to transmit packets without decoding anything but headers, and only the headers are standardized and optimized for this purpose. Since campus and research networks carry traffic at very high speeds, there is no practical way to do full-file comparison without seriously degrading network performance. Third, legal and illegal copies of files sometimes are identical. This will become more common as Apple, Amazon, and other companies sell more copyrighted content without DRM.

What about partial signature matching using data from individual packets? In general, even this cannot be done at campus-network speeds, since reading headers does not suffice, and reading anything else slows the network. The larger problem is accuracy: the smaller the basis for comparison, the greater the likelihood of errors, both positive and negative. Compounding the problem, newer peer-to-peer software and other filesharing mechanisms use strong, increasingly sophisticated encryption to protect or disguise files, and therefore to defeat signature matching.

Border and Host-Based Approaches

Two signature-matching strategies might make technical sense. One is more promising than the other, but neither will work for long.

The less promising strategy involves signature matching on users' computers, rather than the network. Over the past few years, colleges, universities, and other networking providers have very successfully persuaded their users to install anti-virus and anti-spam software on their personal computers. Since signature-matching software works analogously, and the target files are already intact, installing anti-infringement signature-matching software might not degrade the performance of personal computers.

Users like and are happy to use anti-virus and anti-spam software because it reduces problems without constraining or suppressing benefits. Unfortunately, much as we might wish otherwise, experience has shown that many users likely would perceive anti-infringement software in precisely the opposite way. If installation of such software were to be required, compliance and technical work-arounds would be-

come major problems. We already see this problem with copy-protected DVDs: users easily and inexpensively replace software that complies with copy protection with software that doesn't.

The requirement might also have serious indirect negative consequences. Users resisting anti-infringement software, for example, might become suspicious of anti-spam and anti-virus software. If this caused a backlash and led users to remove, disable, or bypass those protections, requiring anti-infringement software might not only have failed to achieve its own objectives, but it would also have reversed the Internet-wide security and privacy gains anti-virus and anti-spam software has yielded over the past few years.

The apparently more promising strategy involves the border between campus or dormitory networks and the commodity Internet (that's the regular Internet, as opposed to special high-performance research networks such as Internet2 or National LambdaRail). Commodity connections are expensive, and so colleges and universities typically buy no more capacity or speed than they need. Moreover, all traffic destined for the commodity Internet flows through one or two connections at the typical campus border, so gathering packets seems more feasible than it does within campus networks. As the Committee has heard today, sufficiently fast signature matching therefore might be possible at commodity border points.

But even perfect border screening can succeed only partially and temporarily. For example, it cannot detect or act on filesharing within campus networks. As peer-to-peer encryption becomes more common and powerful, it will become increasingly difficult to identify files. As some vendors begin selling music and movies without DRM, it will become impossible to differentiate legal from illegal transmissions using signatures. False positives and false negatives will increase, thus rendering even border screening ineffective and counterproductive.

5. Technological obstacles to behavior have only limited and transitory effects

I have confined my remarks thus far to technical feasibility. Let me conclude with a broader observation.

Unexpected problems arise in networked environments. In large part this is because fast, extensive networks enable people to do foolish things much faster—and at much greater scale—than they could otherwise. Since colleges and universities started providing high-performance networking to entire communities earlier than anyone else, we have lots of experience assessing and solving problems that arise in intensively networked environments.

An important lesson we have learned is this: When the problems that arise are about personal and organizational behavior, about the rights and responsibilities of community members and citizens, the only successful, robust way to address them is with social rather than technical tools. We must educate people to understand why certain behaviors are counterproductive for their own community or economy. If we do that together—by which I mean owners, publishers, transmitters, and users—collective good will trump individual malfeasance. When we instead restrict behavior technologically, we get nothing but an arms race we can't win.

I hope that this committee can translate this lesson into effective policy and collaborative practice, and I appreciate the opportunity to provide whatever help I can.

BIOGRAPHY FOR GREGORY A. JACKSON

Gregory A. Jackson is Vice President and Chief Information Officer at the University of Chicago. In this capacity he reports to the President, and manages the University's central computing facilities, telephones, communications, network services, administrative computing, academic computing, computer store, and related entities.

The umbrella organization for these activities, Networking Services and Information Technologies, spends about $70 million annually overall. It employs about 350 individuals (not counting students). Jackson also works closely with the University's widely diverse academic and administrative units to frame and guide more distributed information-technology activities, and to make sure the University makes optimal use of information technology in its education, research, and administration. He serves on University-wide committees, councils, and boards including Budget, Computing Activities and Services, Patents and Licensing, Research Infrastructure, Intellectual Property, Provost Staff, Executive Staff, President's Council, and various others.

Jackson has served on the Boards for EDUCAUSE, National LambdaRail, and Internet2. He has served as a member of the EDUCAUSE Recognitions Committee, chaired the Internet2 National Planning and Policy Council, and is an active partici-

pant in the Common Solutions Group and the Ivy+ and CIC CIO groups. He also has served on the higher-education advisory boards for Dell, Sun, Apple, Microsoft, and Gateway.

From 1991 to 1996 Jackson was Director of Academic Computing for the Massachusetts Institute of Technology. From 1989 through 1991 he was Director of Educational Studies and Special Projects in the Provost's Office at MIT. Concurrently with his administrative work at MIT, Jackson was Adjunct Lecturer in Harvard's Kennedy School of Government, and Lecturer in the Harvard University Extension. From 1981 through 1990 Jackson was Associate Professor of Education at Harvard University (Assistant Professor 1979–81), teaching in the University's doctoral and management programs in higher education. He served as one of the founding Directors of Harvard University's Educational Technology Center, which studied the use of technology to advance educational practice. He also served as Assistant Director of the Joint Center for Urban Studies of MIT and Harvard University, a multidisciplinary research organization then operated by the two universities. Jackson was Assistant Professor of Education at Stanford University from 1977 through 1979.

Trained as a statistician, Jackson has taught analytic methods for clarifying decision making, including statistical and qualitative research methods; policy analysis and evaluation, especially in higher education; and computer programming. At MIT Jackson also taught an MIT freshman seminar on the scientific integrity of murder mysteries.

Jackson has worked extensively on evaluation and planning methods in higher education; on research, instructional, and library computing in universities; and on admissions and college-choice issues including the differential impact of financial aid on minority and majority college applicants. He is co-author of two books—*Who Gets Ahead?* and *Future Boston*—and of numerous articles, reports, and teaching cases.

Born in Los Angeles and raised in Mexico City, Jackson earned his Bachelor's degree from MIT and his doctorate from Harvard.

DISCUSSION

Chairman GORDON. We will start now with our questions, and I will begin as the Chair.

Dr. Jackson, you state that the network-based anti-infringement technologies will fail within higher-performance networks. Has the University of Chicago actually tested any of the network filter technologies?

Dr. JACKSON. We have used Packeteer extensively and we——

Chairman GORDON. But I was asking you have you tested the network filter?

Dr. JACKSON. The filter, we are in the process right now.

Chairman GORDON. So you haven't done that yet? You haven't tested it yet?

Dr. JACKSON. We have not done it yet. Correct.

Chairman GORDON. So it is a little hard to state that, it would seem to me, with such certainty if you haven't tested it yet.

Dr. JACKSON. Well, we had engaged, we talked to Audible Magic at length at a conference in the fall.

Chairman GORDON. But you haven't tested it, although you——

Dr. JACKSON. And they had agreed with——

Chairman GORDON.—stated unequivocally that it won't work.

Dr. JACKSON. Correct, Mr. Chairman.

Chairman GORDON. Okay. And you have also said that technological obstacles to illegal behavior have only limited and transitory effects. Do you believe this is true for spammers and computer hackers and people who develop computer viruses? And if so, why does the University of Chicago use anti-spam, anti-virus software and firewalls, and why should illegal filesharing be any different from these other illegal activities?

Dr. JACKSON. Well, let me say two things about that, because that is an excellent question.

The first is that spam and virus filtering actually work very well because they run on people's own computers, and they run in a way that really doesn't interfere with anything else. So people do not perceive any problem from doing that.

Chairman GORDON. Are they 100 percent effective?

Dr. JACKSON. They are pretty close to 100 percent effective. Yes. Up in the 80 to 90 percent effectiveness. If, I should say if we could have a tool that we could persuade people to install that would run at that level of effectiveness and do the filtering accurately, we wouldn't have any objection to that. We have not seen that yet.

The second issue is why we believe that we have been able to persuade people to do this technologically but not to do the other, and the truth is it took us several years to persuade people that they actually should install this, and the key thing is, unless people are very good about their passwords, are very good about not sharing them, are very good about not letting their kids use their machines, and a variety of other problems, all of the anti-virus, anti-spam stuff is ineffective. We have had very good success finally getting people to not share their passwords and not share their machines, and that is purely behavioral influence.

Chairman GORDON. I don't want my time to run out here. You raised a question that was similar to Dr. Sannier, and that is if there is an arms race, where does it stop? I think to some extent we have seen this with spammers and others, and hopefully as you say it has been somewhat successful.

Mr. Ikezoye, could you address your thoughts on this arms race?

Mr. IKEZOYE. Yes. Clearly the ingenuity of the people developing these applications, these peer-to-peer applications, have provided a real challenge technologically but just as these networks have evolved from the early days from Napster to today, also our own product continues to evolve as well. And so I really do think that analogy of comparing these to the spam and anti-virus programs is a good one. In fact, spam and anti-virus both use these registries of content, and we use a registry of content. It just happens to be that we have copyright works in our database.

But where I would, I think, agree with, echo the panel is that I think technology by itself is never going to be the solution and that it needs to be combined with an educational process in that two things, technology, as well as education, go a long way towards influencing behaviors, which is what we have to do to really have an effect on this.

Chairman GORDON. And Dean Elzy, one of the things we have heard as we are trying to get information on this is that when trying to use technology to reduce this illegal filesharing, you really can't install it on every computer on the campus, so that makes it more expensive or more difficult. What has been your experience in that regard?

Ms. ELZY. We have been looking at technologies that will impact all of our students and all of our faculty and staff as opposed to just the residence halls and some other areas. So we are looking at more global opportunities to install both filtering and education technologies and software that will take care——

Chairman GORDON. Have you found that the vast majority of the filesharing was from the residence halls?

Ms. ELZY. Yes, we did. Some of our early studies and snapshots that we have been able to do over a period of the last 18 months have shown that by far the majority of the filesharing is done, in the residence halls.

Chairman GORDON. I think it was 97 percent.

Ms. ELZY. Ninety-seven percent of the filesharing that is happening is there, but only 27, 26 percent of the computers on campus are doing any filesharing at all. So it is 97 percent of 26 percent. So it is a much smaller percentage than we expected to find.

Chairman GORDON. So that, again, if we are playing hand grenades, and we know we are not going to get 100 percent, that would be a more economical way to approach the problem for universities.

Ms. ELZY. Absolutely.

Chairman GORDON. Thank you, and now I call on Mr. Hall.

Mr. HALL. Thank you, Mr. Chairman. It seems to me that the panel agrees substantially on a number of important issues from the testimony we have just heard and from the testimony you submitted.

I would like to take a moment just to make sure I have got that right. Does everyone agree that technology can't completely stop piracy? And next, does everyone agree that notwithstanding its imperfection, technology can be a part of a comprehensive anti-piracy policy? I never saw such an agreeable group.

Dr. Jackson, in your testimony you described the principle challenges finding "the elusive right balance between mechanisms to protect intellectual property and mechanisms to make it accessible. Tradeoffs are inevitable." So it appears that the broader community has entered into a number of cooperative projects on this, including Dr. Elzy's Digital Citizen Project and the Joint Higher Education and Entertainment Industry Committee.

Dr. Jackson, do you believe these groups can provide the information your institution needs to make informed decisions about comprehensive anti-piracy efforts?

Dr. JACKSON. I believe they are on the right path to doing that. We participate in the Joint Committee, and that has been a really useful place to come to common ground, I think. I mean, in a sense there has been better discussion on the technological pieces than on the educational pieces. So each of us is doing our own educational thing, and it has been much harder to find a coherent campaign that we can all do together that will really help students understand that they are shooting themselves in the foot.

Mr. HALL. One day you think there will be technology that will do that?

Dr. JACKSON. I don't think there will ever be technology that will do it perfectly. It is interesting. If you look at spam and viruses, viruses we have pretty much won the battle against viruses. Spam, most of us who run large E-mail systems believe we are losing that battle, and that within the next year or two we will have lost it completely.

Mr. HALL. Do the other panelists agree that vendors, higher education, and the entertainment industry are making some progress in this area? Anyone care to comment on that?

Dr. SANNIER. I think that——

Mr. HALL. The progress you are making.

Dr. SANNIER. I think it is clear that we are making a significant reduction. I think that all the panelists agree that this is an evolving issue that the technologies that sharers are using will require escalating counter measures in that arms race that I referenced, but that also the industry itself is making progress. Probably the most significant technological advance or advance of any kind in this area is the introduction of the ability to purchase rights-free music, that meets consumers' demands. That more than anything else will reduce the demand for illegal filesharing by providing an excellent legal alternative.

Mr. HALL. Dr. Elzy, I mentioned you in my question. What is your opinion on the progress that has been made?

Ms. ELZY. I think there has been a significant amount of progress, particularly because we have been able to talk to different groups and get different people to the table that haven't been before. I think evidence of the improvement that we are seeing is that the entertainment industry itself is taking great strides. One of the ways that a lot of the monitoring systems will find digital files is through some sort of electronic signature on the file, and for example, we have seen an increase of 40 percent in how many of the files are signatured. The caution here is that the music industry has gone from 11 percent to 51 percent files found. So we can only find one out of two illegal file transfers. The electronic file signatures for movies are almost non-existent, and you can't stop what you can't find. So we are hoping that the entertainment industry will continue its efforts to try to individualize their files so that the tracking systems can actually be more accurate.

And as they become more accurate, then higher education is going to be much more ready to adopt them.

Mr. HALL. You know, we haven't talked about expense and the cost of that technology. Maybe there is no good comparison here, but 15 years ago E-Systems, a company that had national and international operations, had indicated that they had technology that could protect our border, but it was too expense. And now here 15 years later they are talking about building a 20-foot wall or putting the National Guard down there to lock arms on it and question what kind of expense that is going to take. And they don't think that is going to be too much if it takes that to protect the border. And do you feel that we ought to go to that expenditure if it takes it to stop the piracy? I am sure you all agree that we should, don't you? Do you not?

And I am not going to ask you where is the money going to come from, because I think you all have a good idea about that.

My time is up. Thank you, Mr. Chairman.

Chairman GORDON. Thank you, Mr. Hall.

Mr. McNerney is recognized.

Mr. MCNERNEY. Thank you, Mr. Chairman. I am afraid I am going to overrun my five minutes, so you will have to hold me back a little bit here.

I thank the panel, I think this is a very fascinating discussion, and there is a lot to learn here. One of the things that Dean Elzy said impacted me personally; my own children were in college recently, and then the arrests were made, and that definitely makes an impression on you, and so I wanted to make sure today that I get things as straight as I can.

Dr. Wight, I was very impressed with——

Chairman GORDON. I am going to clarify that it wasn't your kids that were arrested.

Mr. MCNERNEY. Oh, no. They weren't the arrested, thank goodness.

Dr. Wight, I was very impressed by your approach you are using, and I think that is probably common here. You are using the technology to the ability that you can, but you are also using the people in responsible positions in your university to make sure that the law is followed. And that must mean residence monitors and people at different levels—are they as willing to participate in this, or is there feedback? It seems like that is an opportunity for abuse at some level that would put people at risk that may not want to be in that position.

Dr. WIGHT. This activity is centered in the university's information security office, and we only deal with about two or three instances of suspected abuse each week. So it is a part-time task for one person in our ISO office, and it is not that big a deal. So we don't get non-technology people involved in the process but when something occurs, somebody from our ISO office goes and visits with a student or a computer user and makes a detailed assessment of the situation. And that is really necessary because it is not possible to tell with a 100 percent reliability if a suspected case of copyright abuse was actually legitimate or not.

Mr. MCNERNEY. Well, one of the things you mentioned was, I think you said two gigabytes. If there is two gigabytes downloaded in a day, then that account is identified in some way. Do you stop the transfer of data during the process, or do you wait until the process is finished and flag it and then confront the person, or how does that work?

Dr. WIGHT. We stop that process immediately, automatically. It is a network switch, and usually the next day somebody from our information security office follows up with the user to figure out what was going on. There are only two cases that I know of where we cut off a student's network access inappropriately. In both cases they were using voice-over IP software to talk with their parents and their grandparents, and what we did was we restored the network access and actually raised the threshold for those two students so it wouldn't happen again.

Mr. MCNERNEY. Thank you. Dr. Sannier, I am sure I am not pronouncing your name correctly, but I was interested in this Ruckus software. That is something that is available to the university to download films and music and so on, but Dr. Jackson raised a good question. If you go legitimately to Microsoft or Apple, you can't share files. Does Ruckus get around that problem? Does it allow students to play on different platforms and so on?

Dr. SANNIER. All of the services that you subscribe to, sir, have these liabilities, because digital rights management software is still

in the cumbersome stage. And so each of these systems has their own particular idiosyncrasies. So once you have adopted a system, they can service very well, but we are still not at the stage where the services that consumers can purchase or that we can purchase on behalf of our students are meeting consumer demand. And I am hopeful that technological advances in the next two years or so will greatly reduce this problem by reducing the demand for piracy because the commercial services will begin to meet the demand.

Mr. MCNERNEY. So you are doing a carrot-and-stick here, and then you are going to put technology in place, you are going to punish bad doers, and then you are going to offer something that will work maybe as well as illegal, maybe better than illegal transfers.

Dr. SANNIER. Absolutely. It seems that that coordinated approach, I think you see everyone on the panel agree that, you know, that is the method by which this problem will get contained and ultimately solved.

Mr. MCNERNEY. I have got to ask you a tech question here, Dr. Ikezoye. You gave a pretty good explanation of why your system doesn't interfere with bandwidth and how it works with packets. About how many packets of the initial transfer do you need to make an ID, to make sure that what is being transferred is legal or not illegal?

Mr. IKEZOYE. The first time we see a file, we need to reconstitute, reassemble enough of the file to do the ID, which is about 20 to 30 seconds of a file, whether it is a soundtrack for a movie or a song. But once we do, as I mentioned then we associate that identification with this ID number. It could be like a passport number, that then later on we can get after the first or second packet we could identify that and then block the transfer.

Chairman GORDON. Thank you, Mr. McNerney. And Mr. Feeney, you are recognized for five minutes.

Mr. FEENEY. Well, and I will thank you, Mr. Chairman, for having this hearing. I am one of at least three members of this Committee that is also a member of the Judiciary Committee. I can tell you that we take property rights, especially intellectual property rights very seriously on that committee. We focus on that.

Now, this is the third committee by the way, the Labor and Education Work Force Committee has held hearings on the technology involved in the universities because this is a huge problem, and Congress is going to continue to focus on it. I should tell you that as an old real estate lawyer, I never tire of pointing out that most Americans think of property rights with respect to the home that they own, and land that they may own as a business, but it was only as an afterthought in the Bill of Rights that the founding fathers got around to memorializing our specific rights to hold our real property. It was in Article 1, one of my favorite articles as a Member of Congress, that the founding fathers pointed out the critical nature of protecting intellectual property.

And while I appreciate the, you know, the panel's recognizing the importance of intellectual property and I want to agree with everybody that education is key, but education alone cannot solve the problem. I am disappointed, I guess, to some extent that Dean Elzy and Dr. Jackson have minimalized the possibilities and the importance of technology in this regard, because while I am sure you

educate your students, Dr. Jackson, on the importance of not committing robbery or burglary or rape, you also put locks on the door. And sometimes the only way to help young people learn the importance of respecting civil institutions, some of the responses you gave about how you can't change behavior until you change culture, et cetera, remind me when I went to China and pressed the issue of intellectual property. We have got rampant theft in China and some other countries around the world.

The commerce, the equivalent of our Commerce Secretary, he was a very brilliant guy. I believe he is educated in the U.S., perhaps even the University of Chicago, because he could have taught economics. He was a real free market kind of guy. I was very impressed. But his answer was very similar. He said, you know, this can be a long process in China because it is going to take us decades to change people's attitudes and behavior.

And I guess the point of all this is to tell you that the Judiciary Committee, see, on a bipartisan basis it is not going to be patient for very long with universities that haven't made aggressive steps, including education, including policy, including technology, whether you like it or not. And we are not going to tell you which technology to use, but I think I speak in part for Chairman Berman, who chairs the Intellectual Property Subcommittee, Chris Cannon, and many others of us when I tell you that our committee is going to be insistent that the universities, not just because of the theft involved, but because you are shaping not just academic excellence for young people, but also their attitude towards civil responsibility, that we are going to be insistent that we reward universities that are aggressive in this regard. I want to note that, for example, the University of South Carolina, Michigan State, Howard University, Seton Hall, Ohio have adopted technological educational, and policy processes that have been very successful. The University of Florida, my home state by the way, talking about the cost, brags about the fact that implementing a technology that they use has saved them some $2 million in expanding the broadband that they had originally intended to do.

So there are potential savings for the university networking opportunity when you diminish the theft.

And I guess with that, because I have got a lot more experts on the panel than I have expertise in this regard, I did want to issue that very important statement. I would ask, you know, perhaps Dr. Jackson and Dr., Dean Elzy, because I did single you out for my disappointment that you hadn't emphasized the potential of technology here.

I guess I would ask you, give you a slight chance to defend your positions. We are spending a good deal of federal resources in terms of helping universities with their technological improvements directly and indirectly through student funding, et cetera. Is it responsible for a Congress that wants to protect intellectual property rights to continue to fund network enhancements for universities if some of those enhancements are indirectly being used, in fact, to promote intellectual property theft, and that would allow the two of you or whoever else would like to respond.

Dr. JACKSON. Yeah. If I may, I should say the University of Chicago does use technological means to block things. We are active

users of firewalls. There is all kinds of traffic that we block from off campus. Until Packeteer failed on us we used Packeteer very heavily to turn these things down. So we used technological means to the extent we can.

And I should also be clear. I mean, my job is to make sure that our network is maximally available so that we do the best teaching and research we can. There is all kinds of other use that is going to happen with unused cycles, but any time other use starts interfering with research and teaching, I am not doing my job.

The key thing is that the technologies that we use to keep the interfering stuff from happening have to also not interfere with the critical stuff. So when Packeteer failed on us, for example, it caused all of our commodity Internet, the regular Internet traffic to stop working, and it took us awhile to figure out what was going wrong and to pull the Packeteers out. But this is the kind of tradeoff that is very difficult.

So this is a very important technology for us. We really need it to work, but it needs to work in such a way, this is my point about tradeoffs, that it doesn't tread over into throwing the baby out with the bathwater, if you will. If I gave the impression that we are not fans of using technology to do effective screening, we absolutely are, but I do believe that at this point the technological means available to us aren't going to get this job done. And that we need to go way beyond that, and if we rely on the technology alone, that we are not going to get anywhere.

Ms. ELZY. I, too, would like to share that we believe that technology is a part of the answer, but it is not the total answer, and if we rely on technology too much, we are going to be interfering with the legal uses of peer-to-peer technology and some of the educational activities that we have going on on the campus. For example, there is a lot of filesharing that happens through the course of distance education. There are a lot of my own library files that are digital in nature and may use the distribution technologies that are available to use today. I would like to not have those blocked.

We believe that education can have an impact but only in partnership with all the other things that we have been talking about. And part of the technology solution is getting legal digital media services up and available and comprehensively usable. Approximately 67 percent of our incoming high school seniors, college freshmen bring iPods with them, but Ruckus doesn't work with iPods. So you have a group of students who are disenfranchised unless they switch over to a different MP–3 player or you offer them multiple services.

And when I was sitting in a focus group with a number of students, and I asked them after they had given a presentation on illegal sites and how the students use it, everybody does it, that kind of thing, I asked them to name a legal media service for me, and they couldn't name one. So there is a huge marketing and business opportunity here to get these into the knowledge base of the students. They said they would use the legal services if they knew what they were, if the music was free, and if it had the tunes that they wanted.

Chairman GORDON. Thank you, Dean. Mr. Feeney, we are going to let you join us or join Mr. Sensenbrenner on the next committee, our next panel.

Mr. Wilson is recognized for five minutes.

Mr. WILSON. Thank you, Mr. Chairman. Just a question broadly but I understand that Ohio University, which is in my district, has recently implemented some innovative procedures to fight illegal filesharing. How much do universities communicate with each other in regard to resolving these kind of problems?

And secondly, have you set up any formal pathways of communication to do your plan for in the future?

Dr. JACKSON. Well, here I am at the end. The answer is we communicate extensively on all kinds of issues, but this has been very, I mean, security, research computing, filesharing have been very high on all of our lists for awhile. To tick off a few of the mechanisms, the Joint Committee that was mentioned several times already has been a really effective compact medium, I mean, a few of us sitting in a room, EDUCAUSE, which is the umbrella organization, and Higher Education has a whole set of activities designed. I mean, if you look at the program, there is a huge fall conference where everybody goes. So there is a lot of the program and a lot of the side conversations that are about this.

We trade notes all the time.

Mr. WILSON. Good.

Dr. JACKSON. And this is really important, because it is the only way that you learn, I mean, to take the Chairman's point earlier, one way for us to find out if things work is to sort of try them. The other is I can go to one of our peers that is very similar to us and see what they have done, and if they have succeeded, I am going to adopt that. And we do these kinds of things all the time.

So it is a lot of communication about the technological opportunities and limits, and there is an increasing amount of communication about whether it is poster campaigns or other kinds of educational campaigns that we can do.

One interesting comment, I am not sure I should make this comment, but I will anyway. In terms of enforcement, one of the problems we have is that we will, you know, we have a set of students who have gotten into trouble doing this. And one of the things that is useful to make a point is to make sure the rest of the community knows that folks have gotten in trouble doing this. So public hangings, if you will.

And here curiously enough we run into the *Family Educational Records and Privacy Act,* which is a federal law that says we cannot disclose this kind of thing publicly. My hope very often is that a student who we busted and put through the process will go to our student newspaper and complain, because then the student newspaper will publish it, and we get exactly what we want. But it is this curious game we have to play to try to sort of prod them to ask us a question.

Mr. WILSON. It is a difficult situation, and we feel badly about what has happened in Ohio. We had a situation like this a couple of years ago where even some Social Security numbers of alums got out, and it was a real difficult situation. So I was just hopeful that the communication was going on between the universities, that we

didn't not apply ourselves to make sure that everybody was going to be safe from it.

That is all I have, Mr. Chairman. Thank you.

Chairman GORDON. Thank you, Mr. Wilson.

And Dr. Gingrey is recognized for five minutes.

Mr. GINGREY. Mr. Chairman, thank you. I wish our legal experts, our attorneys, were still here, but since I am around Mr. Feeney, maybe he could answer this question for me. I am old enough to remember as a kid that you wouldn't buy all the comic books on the shelf. You would just buy maybe ten or 15 or 20 of them, and when you got through reading them, you would swap those with the kid across the street for the 20 that he or she had that you didn't have. And I don't know really when you cut right to the chase how different that is from sharing these music files.

And I say that but at the same time I am a real stickler and firm believer in the rule of law and warning youngsters as Ms. Elzy and Dr. Jackson said, that you probably can't completely solve this problem technologically, and of course, you all raised your hands and agreed to that, and there needs to be some balance. And I truly believe if you can scare the bejeezus out of them and show what could happen if they are guilty of stealing intellectual property, and appeal to their sense of fairness and fair play, of course, I think in your testimony, Ms. Elzy, you had said that some of the kids come to arrive at the college campus as freshmen having involved, engaged and steal intellectual property since the third grade, kind of like me and the comic books of 50 years ago.

So I don't know exactly how you get to that, so these comments, of course, are not in the form of a question. You might want, any one of the five of you, might want to comment on that, but in regard to a specific question, and Dr. Wight, this was that fair use issue, in your testimony you highlighted the exemption of copyright for certain non-profit education purposes.

I would like for you or any of you to elaborate on how copyrighted works are used in course work on your campus, and if the other witness would like to discuss that as well that would be great.

Dr. WIGHT. So we do use a lot of copyrighted work on our campus for teaching purposes and research purposes, and the Doctrine of Fair Use gives us the limited right to do that free of charge. We can only do it with portions of work, and we have to restrict it to non-profit, educational activities, but we derive huge benefits from the Doctrine of Fair Use in that respect.

More recently the TEACH Act has given us the ability to use digital copyrighted works in our teaching, in our classes, and again, there are limitations to what we can do, there are responsibilities that we have to live up to in terms of educating students about the copyright and how the use is limited in teaching. We have to password protect the digital files so that they can't be released.

So we have a lot of responsibilities to live up to, but as long as we live within the rules, then we are allowed great latitude in using these materials for teaching. And it would be very, very difficult to get along without it.

Dr. SANNIER. I would just like to echo Dr. Wight's emphasis on how important fair use is to scholarly activity of all kinds. And I

think this is why this is such a particularly important issue, that if we were to allow stringent enforcement of copyright to erode fair use, the country as a whole would be much the worse for it.

And so these are complicated issues because to a kid who is looking at the digital filesharing, it does feel like, well, I am just sharing it with my friends, but fair use is when you share it with your friends and family, not your million closest friends. Because it is kind of hard to categorize a million closest friends, and this is the challenge that all of you face in drafting law that keeps pace with this changing technology.

So, again, the weapon that we have is the commercial sector. The market ultimately will manage this for us.

Mr. GINGREY. And I guess my comic book analogy breaks down when it is just a kid across the street, and now this technology would allow the sharing with a million kids across the street. So I do understand that point. Yeah.

Chairman, I didn't have any other questions. I will be glad to yield back at this time.

Chairman GORDON. Thank you, Dr. Gingrey, and I will remind you that you can also share your LPs with folks across the street, too.

Before we bring this committee hearing to a close, I want to thank our witnesses. It has been a very informative hearing. It has been televised, so there are a lot more folks that are listening to this than are up here today, and our staff is all listening, so we want to thank you. I want to let you know that for any remaining or additional statements from Members and answers to any follow-up questions, the record will be open.

And the witnesses are excused. Thank you.

[Whereupon, at 3:20 p.m., the Committee was adjourned.]

Appendix 1:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Charles A. Wight, Associate Vice President for Academic Affairs and Undergraduate Studies, University of Utah, Salt Lake City

Questions submitted by Chairman Bart Gordon

Q1. Have you had any complaints from faculty or students about any of the technologies you are using to reduce illegal filesharing? Were these complaints related to traffic-shaping systems (such as Packeteer's PacketShaper) or network-filter systems (such as Audible Magic's CopySense Appliance)? Has the use of these technologies blocked any legitimate filesharing or interfered with any educational or research work on the campus network?

A1. To the best of my knowledge, there have been only two incidents at the University of Utah in which student use of our campus network was temporarily disrupted as a result of using the network for legitimate purposes. Both instances were cases in which the student was using voice over IP services from the residence halls, and exceeded our bandwidth threshold for automatic termination of network services. In both cases, network services were restored and the threshold limits raised to accommodate the legitimate activities. There have been no complaints from faculty or staff, and no disruption of any educational or research work on the campus network.

Q2. Was the use of Audible Magic's network-filter system controversial on your campus? For example, were staff and students concerned about privacy, academic freedom, or that such systems would slow down your network? Were any of these concerns borne out once the technologies were installed?

A2. Our use of Audible Magic's CopySense appliance is limited to the local area network serving the student residence halls, so faculty and research use is unaffected. The use of the software was not controversial, and there have been no complaints about abridgments of academic freedom. The reduction in network traffic has actually led to a significant speedup of the network for legitimate uses.

Q3. About how much does your university spend on anti-spam, anti-virus, and firewall software per year? How does this compare with what you spend on technologies to reduce illegal filesharing?

A3. For centralized network and e-mail services, the university spends in excess of $50,000 per year on anti-spam, anti-virus and firewall software each year. In contrast, we spend approximately $7500 per year for the Audible Magic CopySense appliance. The network bandwidth monitoring and reporting software that we use to identify high-bandwidth users was created by University of Utah staff. We would use this capability even in the absence of a filesharing problem, so it does not represent an added cost of reducing filesharing activities.

Q4. What is your estimate of the cost savings to your campus from the reduction in copyright notices since installing these technologies? Could you provide us with an estimate of the amount of time and money required to respond to one of these copyright abuse notices?

A4. It takes 1–2 hours of staff time in our Information Security Office to respond to each DMCA copyright abuse complaint received. Since implementing the use of the CopySense appliance, we have experienced a 90 percent drop in the number of complaints, which translates directly to a savings of approximately $70,000 per year in staff salary and benefits costs. In addition, the reduction in network bandwidth costs in the first year saved the university an estimated $1.2M. Network bandwidth charges have decreased over time, and it is not possible to project the increase in filesharing activity that might have occurred in the absence of CopySense. However, a rough estimate of our savings would be in the neighborhood of $1M per year.

Questions submitted by Representative Ralph M. Hall

Q1. Dr. Wight's testimony highlights the exemption of copyright for certain nonprofit education purposes. Please elaborate on how copyrighted works are used in course work on your campus. Does your university employ specific software to allow educational use without risking broader distribution? What is the scope of this type of fair use on your campus and how can educational fair use be differentiated from infringing traffic?

A1. Portions of copyrighted works are used routinely under the doctrine of Fair Use for educational purposes in classes throughout the campus. Usually, this takes the

form of excerpts of published articles or books used to illustrate a concept or to serve as the focus of a class discussion. Our Marriott Library operates a digital reserve section where students can access some of these materials electronically. In addition, some copyrighted materials are used in online classes taught over the Internet. Electronic access to these materials is limited to students in particular classes for limited periods of time, in accordance with the TEACH Act. The Fair Use of a copyrighted work for educational purposes is normally limited to only a portion of the work. Therefore, when access to the entire work is desired, the university obtains the permission of the copyright owner. The Marriott Library uses a variety of technologies designed to limit access to copyrighted works in accordance with licensing agreements and applicable law. These include restricting access to digital resources by IP domain, university network ID/password authentication, and authorization according to particular classes for which students are registered.

Q2. Many of the witnesses described their support for offering students "a legitimate online service, one that provides an inexpensive alternative to illegal filesharing." Does your university offer this service to their students? If so, how many students use this product and what feedback have you received from them? If not, has your university considered their use before? What are the principal factors that affect the decision to provide legal alternatives?

A2. The University of Utah has considered the possibility of contracting with a commercial service for providing low-cost access to music and video files. However, it has no plans to expend state funds or tuition revenues to subsidize a service like this in the near future.

Questions submitted by Representative Michael McCaul

Q1. Do you believe that the availability of a certain technology should automatically legitimize the activity undertaken on it? In preparing students for an increasingly technological world, does it help or hurt them when they are not adequately punished for abusing the school's network and computing resources and privileges?

A1. History shows that advances in technology have consistently outpaced advances in societal norms governing the ethical use of those advances. Because university research is at the forefront of knowledge in nearly all fields, every university has a strong mandate to educate its students and the general public about the ethical uses of new technologies (e.g., cloning, stem cell research, peer-to-peer filesharing, electronic surveillance, etc.). It is only by educating our community about the legal and ethical limits to the use of technology, and by backing up that education with appropriate sanctions for abusing the limits, that we can keep the growth of technology and social norms in balance with each other.

Q2. Is it appropriate for taxpayers to fund school networks that are widely used to facilitate theft? Is it appropriate for school networks—created and intended for academic use—to be slowed and clogged by illegal activity?

A2. No. It is in the best interests of universities to optimize the use of their networks to discourage illegal and unethical activities and to facilitate legitimate uses for education and research.

Q3. We have heard that technological measures exist that reduce or prevent illegal filesharing, reduce the network bandwidth wasted by such activity, secure the network against viruses and spyware, and decrease the amount of time spent by administrators responding to infringement notices. Doesn't the cost benefit of addressing these problems justify the cost of implementing effective network technology? If not, what type of analysis have you used to arrive at your decision?

A3. The cost of eliminating *all* illegal activities on any network would be prohibitively high, and it would raise the cost of higher education beyond the reach of many students. At the same time, the cost of doing nothing is also high, because it would encourage illegal uses of our campus networks that would otherwise be available for education and research. The sweet spot lies somewhere in the middle, by making appropriate expenditures for technologies that reduce undesirable or illegal network activities (e.g., spam, viruses and illegal filesharing) to acceptable levels. Currently, we have spent a modest amount of money ($7500/year) to reduce illegal filesharing by about 90 percent. The administrative burden of responding to infringement notices is currently low (2–4 hr/week), so we believe that our efforts to reduce the problem have been largely successful.

Q4. Rather than purchasing a commercially available technology, some schools, such as Ohio University have used internal technological solutions to block some or all of the illegal music, movies, and software on their networks. Ohio University went a step beyond blocking illegal peer-to-peer programs and shut down a "darknet," which is a private hub that allows students to trade music and movies on the local area network without connecting to the wider Internet. What type of action has your university taken to address the issues of darknets operating on your internal system? What are some of the solutions to finding and shutting down darknets?

A4. All areas of the University of Utah network are continuously monitored for unusually high bandwidth activity, so this type of activity would likely be detected even if files were not exchanged with other computers outside the campus gateway. The Audible Magic CopySense appliance is operated in the portion of the network serving student residence halls, so any registered music or video files shared between computers even inside the network would be detected and blocked. Therefore, the solution implemented at the University of Utah would likely identify and stop any illegal filesharing, even on a "darknet" portion of the campus network.

Q5. Campus officials at Stanford University wrote a letter to students last month saying "Keeping up with the number of filesharing complaints coming in under the DMCA has required almost three full-time Stanford employees." How much time and resources did your institution spend on DMCA notices each year before implementing a technological solution? How much time does your staff spend on notices now that you've adopted a technological solution? What caused your University to take proactive steps?

A5. We currently respond to approximately 2–3 DMCA copyright infringement notices per week, which requires about 2–4 hr/week for a single employee. Prior to adoption of our technology solution, we received about 10 times as many complaints, which required at least one full-time employee to handle. The proactive steps to reduce illegal filesharing activities were taken for three main reasons: 1) to bring students and all members of our university community into compliance with acceptable network use policy and the law, and to educate them on the values of respecting copyrights; 2) to reduce the cost of university network resources by eliminating illegal high-bandwidth activities; and 3) to reduce expenditures on personnel required to respond to DMCA infringement notices.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Adrian Sannier, Vice President and University Technology Officer, Arizona State University

Questions submitted by Chairman Bart Gordon

Q1. Did your campus first test the Audible Magic network-filter system before making a final purchase? Was there a cost associated with this initial testing?

A1. Yes we did test the system prior to purchase. There was no cost to the university during the testing phase.

Q2. You have mentioned that your technical team was initially skeptical about the Audible Magic network-filter system. What were their primary concerns? Did these prove to be well-founded?

A2. The technology to identify and block ONLY copyrighted and otherwise illegal activity is very complex. There was skepticism that the Audible Magic platform could really do this efficiently. There were some initial performance issues with the platform due to the high volume of traffic at such a large university. These issues were resolved and the system is now performing well.

Q3. Have you experienced any significant technical problems since you began using the Audible Magic network-filter system? In terms of reducing the demand for network bandwidth, had it saved your campus money, or do you anticipate that it will?

A3. ASU has not experienced any significant technical problems since implementing the Audible Magic network-filter system. During the few weeks the system was in production during the spring semester, ASU's overall bandwidth utilization to the Internet was reduced by about eight percent (48mb).

Q4. Since installing the Audible Magic network-filter system, have your copyright-violation notices decreased? If so, by how much? What is your estimate of the cost savings to your campus from any reduction in copyright notices since installing these technologies? How much time and money is required to respond to one of these copyright abuse notices?

A4. Since installing the Audible Magic network-filter system, the number of copyright-violation notices has decreased dramatically. ASU went from 247 incidents from January through April of this year, down to 37 during the May/June timeframe. Usually the incidents occurred upwards of a month previously. There were cost savings in a number of areas due to this implementation:

1. University Technology Office Help Desk—significant reduction in time being spent processing violations through the ASU system. Reduction from 45 hours of staff time to 10 hours of staff time which equates to a savings of ~$875 over two months already.
2. Student Affairs Office—significant reduction in time and resources necessary to address student violations. The staff in student affairs must bring in the student to explain the issue and instruct them on good security and copyright protection practices.
3. University Technology Office Network Communications—reduction in bandwidth indirect cost of approximately $8,500 per year. However no direct cost savings have been realized as we commit to a minimum amount of bandwidth per year; our cost per mb is based on that commitment.

Q5. About how much does your university spend on anti-spam, anti-virus, and firewall software per year? How does this compare with what you spend on technologies to reduce illegal filesharing?

A5. ASU spends approximately $80,000 annually for anti-virus. Anti-spam we are using Barracuda Networks devices that total $50,000 for purchase with minimal annual expense, and finally we have approximately 50 firewall pairs with an annual investment of around $150,000. The Audible Magic devices to prevent illegal filesharing cost $100,000 to purchase with approximately $10,000 annual expense.

Questions submitted by Representative Ralph M. Hall

Q1. Dr. Wight's testimony highlights the exemption of copyright for certain nonprofit education purposes. Please elaborate on how copyrighted works are used in

course work on your campus. Does your university employ specific software to allow educational use without risking broader distribution? What is the scope of this type of fair use on your campus and how can educational fair use be differentiated from infringing traffic?

A1. Course material access is restricted to students officially enrolled. All access is technically secured through a single sign-on authenticated I.D. Materials utilized by individual instructors are subject to fair use/copyright provisions. Student redistribution of course material is regulated by the acceptable use policy of the university.

Instructors are provided copyright clearance and assessment of material use through the University libraries resource reserve, central distributed education staff, and college-based support staff.

Q2. Many of the witnesses described their support for offering students "a legitimate online service, one that provides an inexpensive alternative to illegal filesharing." Does your university offer this service to their students? If so, how many students use this product and what feedback have you received from them? If not, has your university considered their use before? What are the principle factors that affect the decision to provide legal alternatives?

A2. ASU offers Ruckus on campus and iTunes (among other services) are available via download from the Internet. There are currently 7,467 ASU users that have Ruckus accounts.

Questions submitted by Representative Michael McCaul

Q1. Do you believe that the availability of a certain technology should automatically legitimize the activity undertaken on it? In preparing students for an increasingly technological world, does it help or hurt them when they are not adequately punished for abusing the school's network and computing resources and privileges?

A1. Changes in technology put pressure on established markets and ways of delivering products. As we have seen, it also puts pressure on our definitions of intellectual property. I think students must be prepared to help the companies they will one day join to adapt to and take advantage of these changes to create value and maintain economic viability. However, ethics training in all its forms is an important component of higher education, and a solid grounding in the value of intellectual property protections to the society that grants them is an important part of that training.

Q2. Is it appropriate for taxpayers to fund school networks that are widely used to facilitate theft? Is it appropriate for school networks—created and intended for academic use—to be slowed and clogged by illegal activity?

A2. Clearly the academic networks run by universities must be focused on the legitimate purposes for which they were created. ASU has been successful in managing our network to ensure that it is not "slowed or clogged" in any way by illegal activity (copyright infringement). ASU's network operations are threatened much more by Spam and Denial of Service attacks.

Q3. We have heard that technological measures exist that reduce or prevent illegal filesharing, reduce the network bandwidth wasted by such activity, secure the network against viruses and spyware, and decrease the amount of time spent by administrators responding to infringement notices. Doesn't the cost benefit of addressing these problems justify the cost of implementing effective network technology? If not, what type of analysis have you used to arrive at your decision?

A3. At this stage we have not observed that the network bandwidth recovered offsets the cost of the Audible Magic solution we have implemented. It is possible that it may in the future, but it is also possible that the solution we have used may not keep pace with the rapid technical evolution of the sharing services, in which case we may be forced to invest in further counter-measures.

Q4. Rather than purchasing a commercially available technology, some schools, such as Ohio University, have used internal technological solutions to block some or all of the illegal music, movies, and software on their networks. Ohio University went a step beyond blocking illegal peer-to-peer programs and shut down a "darknet," which is a private hub that allowed students to trade music and movies on the local area network without connecting to the wider Internet. What type of action has your university taken to address the issue of darknets operating

on your internal system? What are some of the solutions to finding and shutting down darknets?

A4. In addition to commercially available technology such as Audible Magic, ASU uses firewall rules to prevent unauthorized servers on the network. Students are prohibited from connecting any external networking equipment to the ASU network this includes wireless access points; thus restricting using the ASU network for this type of behavior. The Cisco Network Access Control system prevents students from putting unauthorized devices into the network. The networking tools help us to easily notice a rough device for Wireless.

Q5. Campus officials at Stanford University wrote a letter to students last month saying "Keeping up with the number of filesharing complaints coming in under the DMCA has required almost three full-time Stanford employees." How much time and resources did your institution spend on DMCA notices each year before implementing a technological solution? How much time does your staff spend on notices now that you've adopted a technological solution? What caused your university to take proactive steps?

A5. The primary reason for investigating Audible Magic is the time savings in this area. This time savings is not only for the University Technology Office but also Student Affairs. The UTO Help Desk required at least two hours or more to track down the user; complicated incidents would require Netcom or Server support assistance. Once identified, Student Affairs staff the identified party and conduct training classes to instruct the students on correct behavior.

At the rate the incidents were occurring for January through April we would have been on target to address approximately 1,000 incidents over the year. That means at the minimum there would have been 500 Help Desk Hours + 1,000 Student Affairs hours + any additional Netcom staff hours. With the implementation of the device we have already seen a greater than three-fourths drop in the number of incidents. The Audible Magic device may not catch every offense but it is greatly reducing the issues. We will have better numbers after the students return in the fall.

ASU has been taking proactive steps in this area since it became an issue in the beginning of the decade. It has required steady investments of time and resources, and our counter measures have had to evolve in complexity and sophistication.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Vance Ikezoye, President and CEO, Audible Magic Corporation

Questions submitted by Chairman Bart Gordon

Q1. How much does it cost to install and maintain the Audible Magic network-filter system at an average campus? After installing a system, do you continue working with the customer to upgrade and update the system over time?

A1. The cost of our system consists of two parts: the initial purchase of the system and annual charges.

The initial purchase price of our system ranges in price and is based upon the bandwidth of the network it is installed upon. Thus smaller universities generally pay less. This price can be as little as a few thousand dollars to one hundred thousand dollars or more. The installation at one of the largest enrollment universities in the U.S. was around one hundred thousand dollars. Our average sale to universities is around twenty five to thirty five thousand dollars. In addition, some schools can reduce the cost by implementing the system on just the parts of the network which are the focus of the piracy problem - for example, on-campus housing.

The annual charge is made up of two components: The educational module of our system, which is optional, is priced by the number of users, with the annual cost between seventy five cents and two dollars per user. Secondly we charge a support fee for the customer technical support, hardware support, software updates, and a subscription to access our content, of approximately twenty three percent of the system purchase price. Thus a fifty thousand dollar system would have an eleven thousand five hundred dollar annual support fee.

Q2. Some universities have argued that technologies like Audible Magic's will fail on high-performance campus networks. Do you agree with this technical assessment? If your technology in its current state would not operate on high-performance networks, is it likely to improve in the near future so that it will?

A2. Clearly, high performance networks on campuses pose increased challenges from the level of speed, complexity, and management sophistication, but we have demonstrated our ability to handle a wide variety of customer networks with diverse network environments. As mentioned we have our systems in use on over seventy schools including some very large public universities.

Addressing the question more directly, the general concern of high performance network failures tends to focus on the issue of scalability. In order to address scalability, we simply deploy higher capacity hardware systems on the high speeds networks of some campuses. This hardware is readily available and can be configured to handle the high speeds. The second related issue concerns what happens if our product fails, does it have a detrimental impact on the network? As mentioned previously, our system is not an inline device. Because it is not inline, the failure of the system will not negatively effect the stability of the network.

With respect to the future, we feel very confident with our ability to not only to handle existing networks but for our technology and products' ability to keep pace with the increases in network bandwidth anticipated in the future.

Q3. The majority of U.S. campuses already use traffic-shaping technologies to control their network bandwidth. How is this technology different from network-filter technologies such as yours, and why is it not always effective at stopping illegal filesharing alone?

A3. At a lower level, we share a lot of technology with traffic shaping products. Traffic shaping devices are able to identify data streams by application, i.e., they know the difference between e-mail, web traffic, or peer-to-peer filesharing applications. Our system does that but goes one step further. Our system is able to reconstruct the payloads of the transmissions for filesharing applications. These payloads are files such as music or movies. Upon reassembly and identification of the files as copyright media files, we are able to match the unknown file with our copyrighted content registry.

The reason that traffic shaping solutions are not always effective, is that peer to peer filesharing applications are constantly evolving and require a dedicated focus to keep up. Because our product is focused on peer to peer filesharing and not any other applications, we are able to ensure the most up to date technology to manage illegal filesharing. In addition, traffic shaping technologies affect all P2P traffic, both legal and illegal. With the CopySense solution, only the illegal P2P traffic is affected.

As an aside, our technology has been designed so that it could be integrated very easily into traffic-shaping or other advanced routing network infrastructure devices that currently exist on most networks today. As an example, our technology can even be integrated into the network infrastructure of an ISP.

Q4. Your technology includes a database of the fingerprints of copyrighted music and movies, and is one of the largest in the world. How quickly is the database updated when new songs and movies are released?

A4. Our database is updated on a daily basis. In many cases, due to our relationships with the content industry we are able to update the database with new songs and movies before their commercial release.

Q5. You mentioned that your product can be configured to be consistent with different universities' privacy policies. Can you explain in more detail how this works? Are technologies such as yours any more invasive of privacy than anti-virus or anti-spam software?

A5. Privacy policies vary widely from university to university. Some universities want to restrict the data on system reports that include IP addresses of individuals. We have designed the CopySense system so that it can be configured to restrict access to information in a manner consistent with a university's privacy policy. If so configured, the university could treat this system as a black box as they do their other network equipment. This black box operates automatically without access by unauthorized personnel. In some cases if a school's policy is that no university personnel can access activity information, the system's educational features could be configured so that only the student is notified of detection of their inappropriate behavior.

The analogy of anti-virus or spam filtering products is an appropriate one. Our products operate in a manner similar to anti-virus products or even spam filters—only our registry contains fingerprints of copyright works rather than fingerprints of viruses or spam. An additional protection to privacy is that our system matches only copyrighted items in a database that are transferred over known public filesharing networks. All other communications such as e-mail and web traffic go by unimpeded and without inspection.

From one perspective, our product is much less invasive from a privacy point of view than spam filtering technology. Our product only detects the transfer of copyrighted works over public filesharing networks. Remember that these networks connect millions of anonymous strangers who are revealing the contents of their computers' hard drives; it is a question if there is even an expectation of privacy under these circumstances. Contrast that with spam filtering technologies, which scan and intercept private e-mail communications between known individuals.

Questions submitted by Representative Ralph M. Hall

Q1. Many of the witnesses described their support for offering students "a legitimate online service, one that provides an inexpensive alternative to illegal filesharing." How does the CopySense application differentiate legally obtained copyrighted works on these services from infringing distribution on P2P networks?

A1. Our system only detects content transfers over known peer to peer filesharing applications. The system ignores transfers of content using online legitimate services such as iTunes. Therefore we do not have to differentiate the copyrighted works, we just have to be able to detect and identify the transport mechanism, whether peer to peer or iTunes. As an aside, even copyrighted works legally obtained from a legitimate online service are not legally allowed to be copied on P2P networks.

Q2. What works are currently protected through use of CopySense? Does the database include non-entertainment material such as books or scholarly articles? How do copyright holders add fingerprints of their works to the database? Is there a limit to how large the database can be before impeding the functionality of your hardware?

A2. The database currently handles most of the North American catalog of music and has a rapidly growing catalog of film and television content. At this time, we have not yet created a database of books or scholarly articles.

Copyright owners that want to register their content are able to contact us, sign a registration agreement, and then we work with the copyright owner to fingerprint their content in the most efficient manner. Most of the time, this consists of pro-

viding a software program to the copyright owner, which allows them to fingerprint the digital file. In some cases, the copyright owner will provide us physical media and we provide services to fingerprint their works for them. Because the fingerprint database is managed and located centrally, there is no relationship between the size of the database and the size of the hardware installed in the university. Therefore the answer to the question is that the database could grow indefinitely and will never impact the functionality of the hardware.

Questions submitted by Representative Eddie Bernice Johnson

Q1. Some of the other panelists are concerned that technologies to reduce illegal filesharing will slow down networks, especially on large research campuses. Has this been a problem at large research universities where your technology is installed? Will the speed of your technology continue to increase?

A1. In our over 70 university customers, our technology has never been the cause of a slowdown of the network. In fact, because we can significantly reduce the bandwidth utilization of these filesharing applications, performance generally increases. However, technically the reason our technology is not a problem is that our system is not an inline device. Inline devices are problematic since all the data traffic needs to go through them. If the device is not fast enough or even worse, fails, it can slow down or stop network traffic. As a device that is not inline, the CopySense appliance operates on the sidelines and performs its matching activity in parallel with the real time network traffic flow. The actual experience of our university customers has been that the CopySense appliance has no adverse impact on network performance.

The speed of our technology will continue to increase with the increases in computational power available in the market. I do not anticipate that hardware performance will be an issue for the foreseeable future.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Cheryl Asper Elzy, Dean of University Libraries and Federal Copyright Agent, Illinois State University

Questions submitted by Chairman Bart Gordon

Q1. Since the beginning of the Digital Citizen Project at Illinois State University, have other universities sought information about your experiences and information on how to reduce illegal filesharing?

A1. Several associations and universities have sought out the leadership of the Digital Citizen Project through a variety of venues. One avenue of contact is through the Project web page at *http://www.digitalcitizen.ilstu.edu/*. Another opportunity for sharing what we've learned so far comes through presentations at conferences like EDUCAUSE. Many will take our cards or contact us afterward once they've attended one of our sessions. The Project's technology specialist and one of the Project's leaders based here in DC gets many calls.

All are seeking advice. Most just want answers—a shrink-wrap solution they can buy and all the DMCA complaints will go away. At present, the Digital Citizen Project doesn't have that answer. We are gaining experience every day. We are documenting the scope of the problem with each new study and data collection. There is much work to be done and improvements to be made before the technology will be effective in stopping the DMCA complaints and eliminating downloading. Some of the answers will come from changing cultures and behaviors as much as relying on a technological monitoring or blocking solution.

The surprising large number of calls and contacts we do get about the Digital Citizen Project and its findings confirms our belief that a National Center on downloading issues should be funded and created at Illinois State University. All of higher education is laboring with a lack of reliable information on what to do, what works, and—more importantly—what doesn't work. Such a Center as we propose could provide reliable, tested, replicable information on products, softwares, educational programs, and more.

Q2. You mention that ISU would like the Digital Citizen Project to be a "consumer-reports-like" study on ways to reduce illegal filesharing. Could you explain this in more detail? How would such a study work and what type of results might it produce? How would you integrate new technology products into the study throughout its duration?

A2. The "consumer-reports-like" study refers to an aspect of our study wherein Illinois State could capitalize on its strong working relationships with multiple associations and vendors to compare and contrast the capabilities of the emerging software and hardware products that are appearing almost weekly. The "reports," as we conceive of them at present, would involve testing each product—first on a test networking and then on a segment of our live network such as a residence hall complex—and determine the effectiveness of the product from a variety of benchmarked perspectives. These elements might include ease of installation, size of the music and movie library, compatibility with Macs and PCs, ability to stand alone versus requiring another software or program to work. While the early focus would be on monitoring systems and escalated response programs, it could easily be expanded to include an evaluation of legal media downloading services or K–12 educational programs.

It is important to remember that many of these products were originally developed for other uses than tracking filesharing but are being adapted to meet this new challenge. Also, in most cases they are products for a commercial environment. ISU is testing these in a live networked higher education environment to identify their strengths and weaknesses for reducing illegal filesharing. Each product will be set up for at least a semester through our residence hall network. Results expected vary depending on the sophistication of the product but may include: does the product identify copyrighted downloads and stop uploads, can the product tell the difference between copyrighted and non-copyrighted material, how much of downloads are being missed, and does it recognize metadata.

It is also important to note that some of these products can be tested on a live network while others absolutely cannot. Certain programs cannot because their technology needs to alter the make-up of the ISU network so drastically as to make the ISU network profile so different that it could potentially change daily academic and business uses of the live ISUNet network or bring the network down all together. (This highlights a crucial reason that independent testing and evaluation is

sorely needed by higher education. No institution can afford to destabilize its network in installing a product, nor can it change its network architecture to meet the demands of a new technology.) For those not able to be on a live network, a test network is essential, so Illinois State is seeking funding to create a small test network to provide a safe environment for study and evaluation.

When the Project leaders become aware of new products, the new vendor is contacted and invited to join the project immediately. A product can be added at any time.

The timetable for the Digital Citizen Study covers several years. The first phase of the study will be completed in June 2008. Existing funding extends only through that date. At that time we will have completed the early testing of two to three monitoring products, several surveys of college students' behavior and motivations regarding downloading, initial release of an escalated response system just developed at Illinois State, and put in place legal media downloading services. The long term effects of this will not be known because we will have just barely gotten all the elements of the Project started by the end of this first phase. The results of this first phase will be the foundation to build the solution for this problem in the next phase.

We are seeking funding from private foundations, from the entertainment industry, and from the public sector to undertake succeeding phases that include studying downloading behaviors in the K–12 age ranges and developing educational modules for the kindergarten through senior in high school level that will successfully capture their attention and positively impact their behaviors. We believe that through education at this younger level, with technological barriers in place, a long term solution is possible. These educational modules must appeal to the younger generation and be able to be integrated into an already crowded curriculum easily for teachers to incorporate them at point of need. Research in conjunction with Illinois State University's College of Education faculty using our elementary and secondary laboratory schools provides us an excellent opportunity to develop these modules. Moreover, ISU has institutional agreements with seven professional development schools—existing K–12 school districts—throughout the state representing demographics from rural to inner-city, from poor to wealthy. This phase is a three year project.

Other phases of the Project that would get underway concurrently include further testing of monitoring systems with feedback both to industry and vendors as well as higher education decision-makers, exploration of financial models that might make systems on campuses more affordable and defensible, development of better public relations programs through a clearinghouse exchange of successes and best practices with other colleges and universities, and a comparison of existing educational programs available throughout the marketplace.

The biggest barrier to Digital Citizen Project is money and time. Money and time. The work undertaken is labor-intensive, uses a lot of expensive technology, and requires a wide spectrum of expertise from network engineering to behavioral research to effective marketing to classroom excellence. Without additional funding, the Project will begin shutting down in March 2008. With additional funding, the Project can expand and adapt as rapidly as the downloading issues themselves.

Questions submitted by Representative Ralph M. Hall

Q1. Dr. Wight's testimony highlights the exemption of copyright for certain nonprofit education purposes. Please elaborate on how copyrighted works are used in course work on your campus. Does your university employ specific software to allow educational use without risking broader distribution? What is the scope of this type of fair use on your campus and how can educational fair use be differentiated from infringing traffic?

A1. The Project leaders at Illinois State would certainly echo Dr. Wight's testimony regarding legal, educational uses of copyrighted media. At Illinois State University and on other college campuses, downloading and peer-to-peer technology is used heavily in distance education applications, in legitimate sharing of data and research through scholarly exchange of information online, in legal software upgrades for important programs such as Linux, for digital files housed in the university's library and shared for class reserves, and more. Our course management software on campus is WebCT through which students access many of the course materials, syllabi, and other course-related documents. WebCT allows faculty to post (with copyright permission) electronic journals, digitized chapter in books, images, film clips, audio files, and more—all with password protection so only authorized students can access the items. All these legal uses of downloading technology must be protected.

To do less would be to cripple the academic enterprise. That is one of the many reasons that Illinois State chose not to block peer-to-peer traffic unilaterally.

Illinois State University has, for almost seven years, used Packeteer to shape the traffic on our network and give highest priority for academic and administrative purposes. The university's library and campus technology's working groups have developed methods for password-protecting files from images to film clips to electronic journal articles to data files so that only a given class or other specified group can gain access to material available for legal use through copyright permissions.

The Digital Citizen Project's leaders feel strongly that the faculty model the behavior adopted by their students. If a faculty member bootlegs an opera or a play or a film, then the students will think it must be okay. We must make legal use of films, music, and all digital media easier by creating better avenues for securing copyright permissions. This can be illustrated with an experience straight from the Project's history. We were creating a brief training session for all incoming freshmen about the dangers of downloading and the fact that not "everyone does it." We asked RIAA to help us in getting permission to use a couple of minutes of a copyrighted music video popular at that time. We started the process in April, and in August we still could not get that permission—even with the help of the industry's own association! We must develop and adopt distribution systems that make it easier for faculty to open a computer file and have a legal copy of a film, show, or song delivered to a classroom than it is for that faculty member to bring in his own copy for classroom use—a practice not presently permitted under DMCA.

Q2. Many of the witnesses described their support for offering students "a legitimate online service, one that provides an inexpensive alternative to illegal filesharing." Does your university offer this service to their students? If so, how many students use this product and what feedback have you received from them? If not, has your university considered their use before? What are the principal factors that affect the decision to provide legal alternatives?

A2. Illinois State University has, in the course of the Digital Citizen Project, explored formal agreements to provide legal media downloading services. We even got to the point of negotiating contracts with two different services, but those were never signed. Two crucial factors halted that initiative.

First, the commercial legal vendors have come and gone so fast that it's difficult to be assured the deal is the best one or that the company will still be in existence at the end of the contract. One company with whom we negotiated changed its business model five times in 15 months—from costing $40,000 for our campus and requiring a formal contract to being free and open to anyone with an .edu e-mail address. Further, there are still no solid services with a broad and deep film library. ISU will be approaching Blockbuster and Netflix this fall about creating a college program with us, but that's still speculative.

The second factor is driven by our study of high school seniors coming to Illinois State as freshmen over the last two summers. In summer of 2007, 80 percent of respondents report they are bringing an iPod to campus. iPods still only work with Apple compatible services, and the only legal Apple service is iTunes. The leading campus companies, most notably Ruckus, are not compatible with iPods, so to secure a single service would be to disenfranchise the vast majority of our students.

Instead of bringing one or more legal services to campus, the Digital Citizen Project proposes to inform students—almost relentlessly—about all the legal media services we can identify. Anecdotally, when one of the researchers asked Project focus groups to name one legal service, no one in the groups could. They even thought iTunes was an illegal service. However, the students in the focus group universally said they would happily use legal downloading services if they knew what they were—and if they were easy to use, free or inexpensive, and had the library of songs and movies they wanted. There is a huge marketing opportunity here. If we can point the students in the right direction and find a funding model that may work for the individual and for the University, then we may be able to begin a slow shift in downloading behaviors.

Q3. You state in your testimony that, "if Congress asks all 4,000 colleges and universities. . .to implement monitoring systems over a very short period of time—from our experience it would seem impossible for vendors to supply our needs." What leads you to this conclusion? In your opinion, how many years would vendors need to overcome these obstacles?

A3. The Project leaders have come to the conclusion that—at this point in time—vendors could not supply or service 4,000 college campuses because, in our opinion, they aren't ready. This is based on the experience of the Project itself. For example, Red Lambda is a monitoring system often mentioned in Congressional hearings as

a potential monitoring system to reduce downloading. Red Lambda was the first monitoring system we began working with in October 2004. In January 2005 Illinois State gave Red Lambda $5,000 in installation fees to bring them to campus. Thirty months later, Red Lambda will make its first trip to campus (July 11, 2007) in preparation for installing their program on part of our network for testing and evaluation. When asked whether they have installations beyond the campus where Red Lambda was developed as Icarus, they can name only one or two that are in development or at the talking stage. Audible Magic, at last report, had about 60 customers (both business and higher ed), and they are the industry leader. Other companies like Allot, eTelemetry, Safe Media, and others either have no customers of record or less than a handful.

These systems are also labor intensive to install and maintain. Each and every campus network is different in its architecture, its needs, and its capabilities. Some installations appear to change network settings or registration procedures that can cause chaos on a live network. There is very little available from these companies in the way of technical support either online, in person, or by phone.

The existing monitoring systems that track by individual songs or films also cannot find every copyrighted item. Even the largest libraries of electronically signatured media still only capture 51 percent of the songs (up from 11 percent two years ago, however) and about two percent of the movies. Campuses cannot catch and block what they cannot find. Until the tracking systems are more universal and comprehensive, the technology will not be as effective as the industry hopes.

It should be noted that as monitoring systems become better, so will the efforts to get around them. One of the aspects of downloading that Illinois State researchers would ultimately like to tackle is how long it takes users to find ways to defeat any given monitoring system—whether through encryption or other means. The industry is going to have to constantly change its focus and methods in order to stay ahead of the downloaders technologically—which is why education and changing behavior becomes so much more crucial to reducing downloading.

Should Congress decide to impose a requirement that all college campuses have monitoring systems in place to reduce illegal downloading, the Digital Citizen Project respectfully, but strongly, recommends that campuses be given a generous lead time because vendors will need to gear up significantly to provide systems and support services that will be essential if there is to be any success.

Question submitted by Representative Eddie Bernice Johnson

Q1. You are an advocate that we must educate students about the issue of illegal filesharing. You also mention that most incoming ISU students have already "learned" this behavior while in elementary and high school. What sort of education programs should be instituted in K–12 schools about illegal filesharing?

A1. Illinois State University researchers know that students in the K–12 learning environment today are already far more technologically savvy students than those that have come before them. Many learn from their siblings or peers—or even their parents—very early how to download. Our research tells us some learn as early as third grade, but most know how certainly by their junior high years. With that being the case, our Project is committed to developing interesting and effective educational modules—short technological teachable moments—that teachers could use in the classroom or tech teachers could use in their classes when they are teaching a particular assignment. As one example, imagine a teacher as a class sponsor for a sixth-grade dance group, and the students want to download music from on of the popular downloading sites to use for their upcoming performance. This would be an opportunity for the teacher to take a few minutes to help those young people understand that taking music through an online source is illegal as well as morally unethical. She or he could use one of the many "teachable moments" curricula developed by the Digital Citizen Project that would be fast, fun, and educational. However, at the same time we want to take care to help the students understand that their educational uses of music and media can be fair use while their entertainment uses are not and, therefore, they must pay for them.

Classrooms are already crammed with all sorts of requirements. Teachers are overwhelmed. Educational materials are expensive. If the Digital Citizen Project can develop quick, point-of-use materials that can be woven into any classroom subject or setting, and if those materials are only a click away, and—better yet—if they are free, then there is a much better chance the information will get to the students.

Lessons on illegal downloading can also be incorporated in the many cyber-safety curricula that are available or in development. Being safe and being legal on the Internet are very compatible subjects for discussion in classrooms.

Questions submitted by Representative Michael McCaul

Q1. Do you believe that the availability of a certain technology should automatically legitimize the activity undertaken on it? In preparing students for an increasingly technological world, does it help or hurt them when they are not adequately punished for abusing the school's network and computing resources and privileges?

A1. The Digital Citizen Project leaders believe students should obey laws, appropriate use policies, and other rules for using university resources. The availability of technology should not absolve a user of responsibility for its use. Just as the invention of the match doesn't legitimize burning down a building, the invention of illegal filesharing technology and the audio/video capabilities of a computer don't legitimize stealing music, games, or movies. Students must know the rules and abide by them. In the past we've heard that young people "didn't know" that downloading was illegal. The Digital Citizen Project research has confirmed that, in fact, students DO know downloading and filesharing is illegal—but they do it anyway.

Rather than "adequately punish" students for downloading, the Digital Citizen Project seeks to interweave monitoring and enforcement—the punishment side of the program—with education and behavioral change, while at the same time helping students FIND the legal media services available to them. The Digital Citizen research has demonstrated that punishing them—kids "getting caught"—only has a short term impact on student behavior, and they'll go back to their old habits once memory fades. If the industry and higher education truly wants to solve this problem, then a combination of approaches will be much more effective.

We're facing a long-term cultural change. Think about seat belts. Congress passed the first seat belt laws in 1963. In 2006 seat belt use—something that can save a person's own life—was only at 80 percent. Laws, fines, and other penalties along with some intensive marketing campaigns have only slowly moved people to change their behaviors. Downloading may be just such a cultural change that will take 20 years to effect.

Students must be prepared to function well in today's technologically changing work and home environment. It is education's role, and that of parents, to teach students all through the grades that legal online behavior is essential. This isn't just a college campus issue. Downloading begins long before students come onto campus. A comprehensive answer must be sought.

Q2. Is it appropriate for taxpayers to fund school networks that are widely used to facilitate theft? Is it appropriate for school networks—created and intended for academic use—to be slowed and clogged by illegal activity?

A2. It is appropriate for taxpayers to support computer networks for educational and research functions at all levels of education. Like it or not, without computers and the Internet today, the work of any university would come to a halt. Packet-shaping technology has gone a long way in the last few years to segregate and prioritize a variety of uses of Internet capabilities on campuses. Of the millions of messages and transactions that go across our campus network every day, downloading still represents a very small percentage from the research our project has done.

The Digital Citizen Project is examining a number of funding options that may develop into means of supporting bandwidth for legal downloading by those who actually use it. On ISUNet, our network snapshots have shown that only about 26 percent of the computers on our network engage in any kind of downloading activity. Are there ways that only those who download pay for the privilege? Could there be a "reconnect" fee for those whose privileges are suspended for illegal downloading? Is it appropriate to charge a fee to students much like cable TV is supported? All these are options that are being explored.

Illinois State University has more students living on-campus (and thus using University network resources in their academic AND living spaces) than most campuses due to a two-year residency requirement for all freshmen and sophomores. However, even with such a policy, approximately two-thirds of ISU students live off-campus. While these students do use University network resources while on-campus, much of their entertainment resources come from commercial Internet Service Providers. The point is on most campuses, control and command of University networks only impact a percentage of students' filesharing activity.

We agree with Congressman McCaul that it is no more appropriate to fund networks for theft than to provide them for spam, worms, bank fraud, solicitation, or pornography. Unfortunately, all these things happen on any network. Education, enforcement of policies, and knowledge of how to acquire digital media legally are all pieces of the puzzle to be solved.

Q3. We have heard that technological measures exist that reduce or prevent illegal filesharing, reduce the network bandwidth wasted by such activity, secure the network against viruses and spyware, and decrease the amount of time spent by administrators responding to infringement notices. Doesn't the cost benefit of addressing these problems justify the cost of implementing effective network technology? If not, what type of analysis have you used to arrive at your decision?

A3. The costs of illegal downloading to college campuses are potentially very large. Many hidden costs combine with the more overt or identifiable expenses to add up quickly, especially when campuses receive hundreds of DMCA complaints every year. Anecdotal industry estimates of costs associated with managing one DMCA complaint two years ago were about $1,200. One of the things the Digital Citizen Project researchers want to examine more thoroughly is the actual cost of a DMCA complaint. Initial studies show something much lower than $1,200. Rather, the overt costs are more in the range of $75–$146. Obviously, this needs much more study.

However, the technology to reduce illegal downloading is also expensive. Initial costs for implementing Red Lambda two years ago were approximately $85,000 per year for a campus of 20,000 students. Audible Magic hardware and software costs $50,000 per box with multiple boxes needed to adequately cover campus online traffic. That's just the hardware costs. Ongoing expenses for staffing, maintenance, and other monitoring support activities are significant. Most colleges cannot find the ongoing funds to support that without passing those costs on, once again, to the student. In an age of double-digit tuition increases, campuses understandably are reluctant to raise anything they can avoid.

As described in Question #2 above, Illinois State's researchers are exploring how to make implementing monitoring systems, providing legal digital services, and offering effective education cost-effective. Downloading is an ingrained, cultural way of life for young people today. A lot of factors—including entertainment industry business models and delivery systems—will have to change as we work on the associated problems.

Q4. Rather than purchasing a commercially available technology, some schools, such as Ohio University have used internal technological solutions to block some or all of the illegal music, movies, and software on their networks. Ohio University went a step beyond blocking illegal peer-to-peer programs and shut down a "darknet," which is a private hub that allowed students to trade music and movies on the local area network without connecting to the wider Internet. What type of action has your university taken to address the issue of darknets operating on your internal system? What are some of the solutions to finding and shutting down darknets?

A4. About eighteen months ago the RIAA shared with Illinois State project leaders that they believed about 45 percent of the illegal downloading traffic was happening on "darknets," within the campus network where they could not reach. Illinois State's own network engineers believed that darknet traffic was more like five percent. ISUNet is constantly monitored for unapproved servers or server-like activity, so many felt there was little chance much was happening on our campus in the way of darknets. However, when our Audible Magic box was placed on one floor of one dorm for a brief darknet "snapshot," darknet traffic constituted about 16 percent of the activity. Assuredly, this is a tiny sample, but it is indicative of the need for more extensive documentation so we all can have accurate measures rather than relying on anecdote and supposition.

When our network architecture was analyzed by Audible Magic for ways to address possible darknet, on-campus downloading activity, it was suggested that we needed a minimum of eight boxes (at $50,000 each). 23 or more would be better. No campus is going to undertake such a massive, expensive installation. Internal network monitoring, escalated response with its increasing loss of network privileges for repeated violations, and stronger education have the best chance of combating darknet activity.

Q5. Campus officials at Stanford University wrote a letter to students last month saying "Keeping up with the number of filesharing complaints coming in under the DMCA has required almost three full-time Stanford employees." How much time and resources did your institution spend on DMCA notices each year before implementing a technological solution? How much time does your staff spend on notices now that you've adopted a technological solution? What caused your University to take proactive steps?

A5. Illinois State University has a team of individuals responsible for managing any DMCA copyright complaints. While no one person is responsible and no one has copyright complaints as the sum total of his or her job, many are involved and serve as back-ups to each other. Illinois State has a federal copyright officer, an appropriate use coordinator, a designated network engineer, and several support staff who receive, investigate, identify, notify, and track each individual complaint.

In 2004, Illinois State received 469 DMCA violation notices. Early in its developing phases in 2005, the Digital Citizen Project participants tracked workload and analyzed the costs associated with the DMCA complaints. The cost was $75.26, including staff time, network resources, and any record-keeping for a first offense. For a second offense that would involve the on-campus student judicial process the cost increased to $133.29. In total, then, the 2005 costs ranged from $35,297 to $62,513 depending on the nature of the offenses. In point of fact, it was the increasing number of DMCA complaints and the delivery of four federal subpoenas that began the Digital Citizen Project. We felt we had to do something proactive, something to better protect our students from the possibility of being sued. Yet as a university that firmly stands for and believes in the principals of the American Democracy Project that teaches young people to be good citizens overall and to engage in politics and take civic responsibility seriously, we needed to redirect student behavior and change their culture in this regard.

Illinois State University has not yet implemented a monitoring system, primarily to allow the research of the Digital Citizen Project to go forward without any unusual technological influences. New technologies will be tested this fall after a thorough data capture of network activity has been done. Reports on the effectiveness of the technologies implemented should be available mid-winter.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Gregory A. Jackson, Vice President and Chief Information Officer, University of Chicago

Questions submitted by Chairman Bart Gordon

Q1. How effective and accurate would a technological system have to be for you to deploy it on your campus to reduce illegal filesharing? What technical capabilities would satisfy you that such a system would be appropriate for your university?

A1. Two technical measures are important: how accurately the technology detects infringing files, and what impact it has on network transmission. Accuracy, in turn, has two components—correctly catching infringing files (positive accuracy) and correctly letting legal files pass (negative accuracy). To be useful, a screening technology must have very high positive accuracy (that is, it must catch most infringing files), 100 percent negative accuracy (that is, it must never flag legal files as infringing files), and must have no net negative effect on network performance (that is, its operation must not slow or otherwise degrade network performance, or it must enhance network performance enough to more than compensate for any degradation).

In addition, the cost of the screening technology must not divert resources from core network operations. That is, either the cost must be very low, or it must more than pay for itself by reducing discretionary networking expense.

Questions submitted by Representative Ralph M. Hall

Q1. Dr. Wight's testimony highlights the exemption of copyright for certain nonprofit education purposes. Please elaborate on how copyrighted works are used in course work on your campus. Does your university employ specific software to allow educational use without risking broader distribution? What is the scope of this type of fair use on your campus and how can educational fair use be differentiated from infringing traffic?

A1. We use all kinds of copyrighted work instructionally: library material on reserve, slide collections, films and film excerpts, music, recordings of concerts, and so on.

We use various means to ensure that our use of these materials remains legal. In many cases we get formal permission to use the materials; in other cases we rely on the fair-use exemptions that Dr. Wight discussed.

We use two principal methods to ensure that copyrighted instructional materials circulate no further. In many cases we show them in class rather than distribute them, and otherwise we make the materials available through our campus instructional management system *(chalk.uchicago.edu)* or our central filesharing service *(webshare.uchicago.edu).* Both systems require users to have University network credentials and to be in the relevant class or otherwise be authorized to view and use materials.

Q2. Many of the witnesses described their support for offering students "a legitimate online service, one that provides an inexpensive alternative to illegal filesharing." Does your university offer this service to their students? If so, how many students use this product and what feedback have you received from them? If not, has your university considered their use before? What are the principal factors that affect the decision to provide legal alternatives?

A2. We have considered such services, but have consistently decided not to provide them at University expense. First, there is no subscription-based service that works consistently and seamlessly across different technologies. Ruckus, for example, provides less functionality to Macintosh users than Windows users, and its materials can't be used on iPods; Apple, conversely, will not provide site licenses and insists on charging for each iTunes item, and those items only play on computers or iPods.

Many of our students, faculty, and staff either use free services like Ruckus or purchase movies and music from Apple iTunes, Microsoft Zune, or Real Networks at their own expense. There is no reason for the University to involve itself in these transactions, which are, as they should be, between the vendors of copyrighted materials and their customers.

We regularly ask students whether the University should subscribe to a service, and they regularly tell us they would prefer that we spend on other activities they value more. If an online service were to provide seamless service across diverse de-

vices and to assume liability for any copyright infringement within the University, we might find such a service appealing if only as insurance. But such services do not exist today, and we see no prospect that they will in the near future.

Questions submitted by Representative Michael McCaul

Q1. Do you believe that the availability of a certain technology should automatically legitimize the activity undertaken on it? In preparing students for an increasingly technological world, does it help or hurt them when they are not adequately punished for abusing the school's network and computing resources and privileges?

A1. A few years back our car was stolen. The thieves used Chicago city streets to gain access to the car, to remove it from our premises without permission, and three days later to total the vehicle while being pursued by police. The availability of city streets enabled this criminal act to take place, but did not legitimize it. Similarly, the increasing scope and speed of digital networks enables an immense scale and variety of uses, most of which are legal but some of which aren't; the network no more legitimizes the latter than the Chicago streets legitimized the theft of our car.

In each case—streets and car theft, networks and copyright infringement—we as a society must educate our citizens as to what is legal and why, we must ensure that our laws advance our society, and we must take appropriate steps to apprehend and punish offenders commensurately with their offenses. This is true regardless of what technology enabled the offense. Our focus must remain on the offense and the offender rather than on the conduit involved.

Q2. Is it appropriate for taxpayers to fund school networks that are widely used to facilitate theft? Is it appropriate for school networks—created and intended for academic use—to be slowed and clogged by illegal activity?

A2. High-performance networks, such as those found on most university campuses, are configured and provisioned to handle very high data flows as necessary for instruction or research, even though those very high data flows only happen occasionally. As one of my colleagues pointed out, provisioning data networks is much like managing snow clearance: the network capacity or snowplow equipment is essentially idle most of the time, but when they're needed they must be ready to handle huge loads very quickly.

As a result of this use pattern, it's very rare that copyright-infringing traffic interferes with network operations. The principal exception to this is the border between campus networks and the regular Internet. It's certainly inappropriate for academic resources—be they funded by taxpayers or tuition—to be diverted to non-academic purposes, and that's especially true for illegal purposes. Technological conflict between academic and non-academic use is not common on most university networks, and when it is relatively simple network configuration or management strategies keep everything sorted out.

Q3. We have heard that technological measures exist that reduce or prevent illegal filesharing, reduce the network bandwidth wasted by such activity, secure the network against viruses and spyware, and decrease the amount of time spent by administrators responding to infringement notices. Doesn't the cost benefit of addressing these problems justify the cost of implementing effective network technology? If not, what type of analysis have you used to arrive at your decision?

A3. As I commented above, implementing expensive technologies might well reduce copyright infringement, but given the provisioning of university networks it would not yield any appreciable saving on network operations or administration. There are good reasons to implement reasonable technologies to reduce infringement, but saving money isn't one of them.

Q4. Rather than purchasing a commercially available technology, some schools, such as Ohio University, have used internal technological solutions to block some or all of the illegal music, movies, and software on their networks. Ohio University went a step beyond blocking illegal peer-to-peer programs and shut down a "darknet," which is a private hub that allowed students to trade music and movies on the local area network without connecting to the wider Internet. What type of action has your university taken to address the issue of darknets operating on your internal system? What are some of the solutions to finding and shutting down darknets?

A4. Good network managers monitor traffic patterns throughout their networks, taking steps to understand large flows and to resolve conflicts and choke points. A

darknet that becomes active will begin generating large, detectable data flows. Network managers watch for changes like this, exploring their origin and nature to determine whether the right response is adding capacity or suppressing the flow. None of this is peculiar to darknets or copyright infringement. Video, students legally letting others hear (but not copy) their music collections, Skype, Microsoft patches—all of these can produce unexpected data flows, and trigger responses from network managers. We shut down problematic flows quite frequently, including the occasional darknet and many, many improperly secured computers that have been taken over by outsiders and used to send spam or mount denial-of-service attacks.

Q5. Campus officials at Stanford University wrote a letter to students last month saying "Keeping up with the number of filesharing complaints coming in under the DMCA has required almost three full-time Stanford employees." How much time and resources did your institution spend on DMCA notices each year before implementing a technological solution? How much time does your staff spend on notices now that you've adopted a technological solution? What caused your University to take proactive steps?

A5. I'm baffled by this Stanford statistic. At the University of Chicago the typical DMCA complaint takes about an hour of security-officer time to log and verify, and the discipline process for a first offender typically takes an hour of a Dean's or a personnel officer's time. As I said at the hearing, we expect to receive 100 or so DMCA complaints this year, which translates into 200 hours or of professional handling time, or about 10 percent of a full-time-equivalent professional staff member. If we took no traffic-management steps, that number might double, but even then the total falls far short of the Stanford statistic.

Appendix 2:

Additional Material for the Record

STATEMENT OF MR. SAFWAT FAHMY
CEO AND FOUNDER
SAFEMEDIA CORPORATION

Chairman Gordon, Ranking Member Hall, I want to commend you and your committee for calling this important hearing on "Using Technology to Reduce Digital Copyright Violations on Campus."

My name is Safwat Fahmy, and I am the CEO and Founder of SafeMedia Corporation. Prior to founding SafeMedia, I spent more than 30 years in computer architecture design and software product development. I founded and served as the Chairman of the Board for WIZNET, a business to business ("B2B") e-Commerce content firm and have developed GIS systems for federal and local governments and IBM's IPCS/MAPICS.

My testimony addresses two issues: (1) the privacy risks and other dangers to consumers, students and other users posed by many popular P2P filesharing programs as outlined by a recent report issued by the United States Patent and Trademark Office; and (2) technology developed by my company to address illegal sharing of copyrighted materials on P2P networks. While I understand that the former is not the focus of today's hearing, I believe it is vitally important that the Committee better understands how many popular P2P programs operate as you examine how technology can be used to reduce digital copyright violations on campus.

SafeMedia's mission is to provide an effective, cost-efficient and easily implemented solution for preventing illegal transfers of copyrighted digital material via peer-to-peer networks, and to restore and preserve copyright holders' asset value.

As you know, since 2002, numerous Congressional Committees have addressed illegal piracy on college campuses through peer to peer (P2P) filesharing and the serious privacy and security risks posed by many popular P2P filesharing programs. As early as September of 2002, Congressman Robert Wexler, my home-district Congressman, stated at a hearing before the House Judiciary Subcommittee on Courts, Intellectual Property and the Internet that *2.6 billion songs and 12 to 18 million movies were being downloaded illegally every month.* Perhaps as important as the loss of economic value, is the attendant loss of moral leadership and cultural degradation when intellectual property theft is ignored or even defended.

Starting in March of 2003, the House Government Reform and Oversight Committee held a series of hearings on the threats to privacy and security on filesharing networks. Later that year, the House passed legislation authored by Representatives Henry Waxman and Tom Davis requiring federal agencies to develop and implement plans to protect the security and privacy of government computer systems from the risks posed by P2P filesharing. Among Congress' findings in the Waxman/Davis legislation were the following:

> "Peer to peer filesharing can pose security and privacy threats to computers and networks by—
>
> - Exposing classified and sensitive information that are stored on computers or networks; Acting as a point of entry for viruses and other malicious programs;
> - Consuming network resources, which may result in a degradation of network performance; and
> - Exposing identifying information about host computers that can be used by hackers to select potential targets."

The reality and severity of these risks, to those inside and outside of government, remain today and were most recently documented in a U.S. Patent and Trademark Office ("USPTO") report released last month entitled, *FilesharinQ Programs and "Technological Features to Induce Users to Share."*[1] Researchers analyzed more than six years of data, claims and counterclaims of five popular filesharing programs. The report addressed whether filesharing programs "deployed features that had a known or obvious propensity to trick users into uploading infringing files inadvertently." The study painstakingly examined "technological features" that "induce" users to "share" copyrighted material. In addition to features such as "share-folder," "search wizard" and "partial-uninstall," such coercive features include: (1) redistribution by default—which causes users to "share" all files that they downloaded; and (2) forced-sharing—which compels users to store and share their private folders and documents. which may include copyrighted material such as personal audio files from

[1] *http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf*

paid downloads or purchased CDs as well as sensitive personal information located in consumers' "My Documents" folders.

The report also noted that even if a user is sophisticated enough to understand that he or she has become an unwitting participant in pirating, disabling the features is no simple process. In fact, the report warned that software distributors create, "technological barriers" to ensure that "Disabling filesharing. . .can be very difficult and perhaps an impossible task for all but the most expert computer users."

The Report exhaustively examines how these features were designed and deployed primarily during the period from 2003 to 2006, well after legal actions were being initiated against users. Users, young or older, naive or experienced, are literally laying open their networks and files once they install a P2P filesharing program. The Report also recounts mounting evidence from security companies, government agencies, and television network investigations, demonstrating the serious security and privacy risks posed by P2P filesharing networks. In one example, "a woman's creditcard information was found in such disparate places as Troy, Michigan, Tobago, Slovenia, and a dozen other places. Her music-downloading application was in fact making readily available her entire 'My Documents' folder to that application's entire P2P audience, 24 hours per day." This example and others like it demonstrate why the U.S. Patent and Trademark Office said, "They [filesharing programs] pose a real and documented threat to the security of personal, corporate, and government data."

The Report carefully avoids blaming distributors of P2P software for deceiving consumers, but noted that available public information made clear that their programs utilized such technological features. Incredibly, the companies whose filesharing software USPTO analyzed have not refuted any of the report's allegations. And in the final analysis, does it really matter to P2P networks users whose identity or taxpayer information is stolen or whose legally obtained music has been illegally distributed without their consent, whether the software designers intentionally meant to harm them or did so by "accident?" The simple fact is that the most popular P2P services cannot thrive without "cooperation" from users sharing their files. If that cooperation cannot be obtained willingly, as the report's analysis shows, it will be obtained through "technological features" that "induce" users to "share."

With my background in computer architecture design and software product development, I became acutely aware of the serious privacy and security risks posed by some P2P filesharing networks and the significant economic losses that are being sustained through illegal filesharing on certain P2P networks. I also recognized that technology could serve as an important part of the solution and so in October of 2003, I came out of retirement to found SafeMedia corporation. I understood that any technological solution had to distinguish between P2P networks that utilize seemingly inadvertent and anonymous filesharing and services such as BitTorrent which require identification and consent of peers prior to the sharing of files. I set forth a number of additional criteria for a technologically sound solution and determined that any device or program addressing these issues had to:

- protect user privacy,
- provide 100 percent accuracy with no false positives,
- easily adapt to small or large network environments,
- cause no slowdowns for legitimate network traffic,
- self-correct with no additional administrative burdens to network managers,
- adapt quickly to changes in illegal P2P networks and transmissions,
- install easily, and
- perhaps most important, has to be available at an affordable price.

Mr. Chairman, I am happy to report that after years of hard work, we were able to utilize a combination of breakthrough core technologies to take this effort in a new direction. In fact, our solution will prevent illegal P2P filesharing networks from forming in the first place. We've labeled it "P2P Disaggregator" (P2PD) technology. It can be deployed at end-user sites, either integrated into network devices installed in edge routers/modems or subnet edge routers and concentrators, or as an independent network appliance which I will focus on today.

Our device: "Clouseau" is a network appliance that detects and prohibits illegal P2P traffic while allowing the passage of legal P2P such as BitTorrent and all other Internet transmissions. Clouseau is inexpensive and smaller than a phone book—users simply plug it in between the Internet and their computer network, and it goes to work. With Clouseau, we have addressed and solved the weaknesses inherent in other technological approaches to this problem:

- No Invasion of User Privacy: Clouseau detection does not invade user privacy, never captures or records user IDs, does not decrypt any traffic, and allows the execution of all current security techniques (Tunneling, SSH, etc.). Clouseau never opens packets to determine file legality or illegality. That determination is based solely upon the type of transmission—it never invades user privacy by looking at the content of a file.
- Accuracy: Clouseau is fully effective at forensically discriminating between legal and illegal P2P traffic with no false positives (i.e., identifying another protocol as the targeted protocol) whether encrypted or not. It prohibits sending and receiving all illegal P2P files, and prevents the flow of copyrighted digital files from legal Internet services, DVDs and CDs to P2P networks where they are totally accessible to millions of users to pirate.
- Scalability: With little or no latency and nearly perfect accuracy, Clouseau operates at network speed processing large traffic volumes on the order of several hundred thousands to several million connections at a time (depending on model) with minimal computation expense.
- Robustness: The P2P community is constantly devising new strategies to cloak their activities including launching new protocols, double and triple-layering encryptions, and frequently changing servers. SafeMedia vigilantly monitors all these rapidly changing characteristics. Clouseau is provided with a remotely secure update every three hours ensuring its constant ability to meet these dynamic challenges.
- Network Appliance Advantages: In addition to the above, Clouseau also provides some unique improvements to the appliance model, such as:
    - Lights-Out Management—Clouseau has been designed as a zero-maintenance appliance from the user's perspective. All updates are done automatically and do not require operator/administrative intervention.
    - Network Invisibility—Clouseau operates in a stealth mode when performing P2P filtering. This feature allows the appliance to be completely invisible to attacks that may be launched on the device.
    - Resilient and Self-healing—In the event of physical attack or hardware or software failure, numerous internal fault-tolerant, self-protection measures are in place to protect the device from undesirable changes affecting the appliance's functionality. Should deprecation of the module or corruption of a file system be discovered, Clouseau will self-heal by automatically restoring corrupted files. Clouseau reboots in the event of power loss (in approximately 45 seconds) to ensure system and network security and functionality. Thus, using a combination of resilient operations, self-healing techniques and built-in fail-safes, Clouseau is able to protect itself from multiple types of attacks that may be imposed on it.
    - Plug and Play—Clouseau is very easy to install and requires no changes to existing network topology.

How does Clouseau work? I will do my best to explain in layman's terms the following technologies utilized by Clouseau:

- Adaptive Finger Printing and DNA Markers—SafeMedia's filtering system utilizes proprietary finger printing techniques to identify specific P2P clients/protocols. By using these DNA markers, Clouseau® is able to uniquely identify whether a packet is part of a P2P transaction or regular Internet traffic. By studying the details in-depth, SafeMedia is able to avoid false-positives.
- Adaptive Network Patterns—Not all protocols can be easily identified with single packets. As such, Clouseau® is able to monitor packet flows and adapt its filtering based on what it has already seen and now sees. This extensible system utilizes a technique called experience libraries.
- Experience Libraries—P2P clients and protocols will change every day. The process of adapting to this change and constantly being updated with the latest knowledge of such clients/protocols is the responsibility of the experience library. SafeMedia's network operations trains these libraries with new patterns and DNA markers and push these new libraries to Clouseau® units out in the field.
- Update—No P2P filtering appliance will function without constant updates. All of the methods described above are constantly evolving and SafeMedia utilizes the Akamai network to push new updates through the Internet Using a highly scalable network such as Akamai allows SafeMedia to off-load the deployment of updates to a well-established content-distribution network.

Clouseau has been effectively installed for clients in Florida, California, Oklahoma and Texas in a variety of educational and commercial settings. We are currently deployed at Florida Atlantic University. We continue to expand our higher education efforts and hope to announce soon that we will install the product at a number of additional colleges and universities.

As you know some colleges and universities have been reluctant to adopt effective policies to deal with illegal filesharing. Some cite student privacy as a concern for refusing to stop clearly illegal filesharing, but they need to be challenged with this question: How does it protect student privacy to allow P2P filesharing services to roam student's computer hard drives for private folders and documents without their explicit permission? I would further ask if there isn't a double standard at work. Colleges and universities fiercely protect their own intellectual property. Why are they so cavalier when it comes to the intellectual property of others?

Mr. Chairman, we welcome the insights and assistance that can be given to this issue by the Science and Technology Committee and would be happy to answer any questions you may have regarding Clouseau or the issues that have been raised in my testimony.

REPUBLICAN BRIEFING MEMO

Reducing copyright infringement on campus networks

HEARING OF THE HOUSE COMMITTEE ON SCIENCE AND TECHNOLOGY
JUNE 5TH, 2007 AT 2 P.M., 2318 RAYBURN

The Full Committee on Science and Technology will meet to hear testimony on technologies, available and under development, designed to reduce the movement of copyrighted material across university and college networks.

Piracy of digitally available media has become a large concern as more and more intellectual and creative works are available in easily-transferred, digital format and access to high bandwidth networks has spread. Users can now easily access software allowing illegal filesharing of music, movies, software, and other content. Colleges and universities hold a unique perspective, being both creators of intellectual property and Internet service providers to a large and technically savvy group of students and staff.

A number of other committees have met to discuss aspects of this problem. This hearing will examine one detail of the larger intellectual property enforcement debate, narrowly focusing on the efficacy of technological solutions to stopping illegal filesharing. The witnesses all have expertise on the details of campus networking and various methods that might be used to curtail illegal behavior, including efforts at education and providing legitimate alternatives.

Witnesses

Charles Wight, Associate Vice President, University of Utah, and **Adrian Sannier,** Vice President and University Technology Officer, Arizona State University. Dr. Wight and Dr. Sannier will discuss their campuses' experiences with network-filtering technologies, and what technical issues/concerns remain from their perspective.

Vance lkezoye, President and CEO, Audible Magic Corporation. Mr. Ikezoye will discuss his company's network-filtering technology, and comment on what technical issues may have arisen from its deployment on campuses across the country and what capabilities these technologies are likely to have in the near future.

Cheryl Asper Elzy, Dean of University Libraries, Illinois State University. Dean Elzy will discuss the Digital Citizen Project, a joint project between ISU and the copyright-holder community to act as a live campus testbed for a variety of approaches to reducing digital copyright violations, including network-filtering technologies.

Greg Jackson, Vice President and Chief Information Office, University of Chicago. Dr. Jackson will discuss the University of Chicago's technological and other approaches to reducing copyright-infringing activity on campus networks.

Background

Piracy occurs when an individual unlawfully distributes copyrighted content. As more and more intellectual and creative works are available in easily-transferred, digital format and access to high bandwidth networks has spread, copyright infringement has become a technically trivial process. In addition, while earlier piracy operations were often linked to single servers offering free access to material, today's piracy occurs mostly in distributed networks that lack a central software server. These peer-to-peer (P2P) networks draw on the resources of every computer on the network and cannot be centrally maintained or regulated. While exact data for the amount of piracy is not available, the widespread use of P2P programs suggests a significant amount of infringement.

In responding to piracy, colleges and universities are treated in a like manner with commercial Internet service providers. Under provisions of the Digital Millennium Copyright Act (DMCA), colleges and universities are exempted from liability for copyright infringement on their networks as long as they appropriately respond to notifications of unauthorized distribution. Earlier this year, the Recording Industry Association of America, RIAA, released a list of the 23 schools that the record industry had sent the most notices to, alleging infringing activity by students or staff. A few weeks later the Motion Picture Association of America, MPAA, produced another list, detailing the 25 institutions that received the most notices from their member companies. Both lists are included at the end of this document. While the

methodology has been criticized by some schools, these events have served to highlight the continuing problem of piracy on both campus and commercial networks.

Joint Higher Education/Entertainment Industry Committee

Recognizing piracy as a serious and continuing issue, representatives from colleges and universities and the recording industry first met in late 2002 as the Joint Higher Education/Entertainment Industry Committee (Joint Committee). The Joint Committee was formed to allow content holders and higher education, (1) to examine ways to reduce the inappropriate use on campuses of P2P filesharing technologies, and (2) to explore the prospects for narrowing their differences on existing and proposed federal intellectual property legislation. A summary of the actions of the Joint Committee can be found at the end of this document. In October 2006 and again in April of 2007, technology experts representing members of the Joint Committee and software vendors met to refine requirements for filtering illegal traffic from campus networks. A consensus document detailing the readiness of current technology and remaining obstacles is expected in late June, 2007.

Current Technology

A number of vendors have proposed or developed technologies that may aide network administrators in their efforts to combat piracy. These technologies generally fall into three categories: 1) network filtering, 2) secure, legal distribution, and 3) legitimate alternatives.

Network filtering technologies use various methods to identify and stop network traffic that carries copyrighted data. A number of companies offer different products in this area. These include tools that slow large downloads to deter piracy, that block all P2P activity without consideration of content, and those, like Audible Magic, that attempt to identify content as copyrighted. The witnesses will each discuss costs and benefits to various approaches. Surveys have shown that over 80 percent of colleges and universities engage in some type of filtering or blocking.[1]

In addition to filtering out copyrighted material, colleges and universities must also allow legal distribution of copyrighted content. In particular, educational use of digital articles, books, films, and music is allowed and essential to higher education's core mission. Again, various vendors have technologies to provide students with course materials without risking wider, unauthorized distribution.

Finally, the commercial market for legal procurement of digital media is growing. In addition to widely known businesses like Apple's iTunes and Amazon.com, smaller companies have created entertainment packages that directly target colleges and universities.

All three of these classes of technology significantly interact, with both positive and negative effects. The availability of legal alternatives poses challenges to filtering technologies to allow their content, while blocking others. Alternately, the availability of a secure distribution system for course materials may enable network administrators to filter out infringing activity more easily.

Digital Citizen Project

The diversity of products proposed or currently available to colleges and universities to combat piracy presents opportunities and challenges. Network administrators may find integrating separate systems within the campus network particularly difficult. However, administrators also have wide latitude to choose products that meet both the technical and policy requirements of their institutions.

One specific barrier to further implementation has been a lack of data on the effectiveness and utility of various vendor technologies. Illinois State University has embarked on a project specifically designed to evaluate these technologies and disseminate their results to other higher education institutions.

The Digital Citizen Project began in January, 2007 and aims to use,

> *a comprehensive approach to confront pervasive attitudes and behaviors in peer-to-peer downloading of movies, music, and media we address ethical and legal issues through the following: educating our college students, self monitoring and enforcement, providing multiple legal digital media services, marketing and public relations of our program and services, investigating K–16 use of peer-to-peer*

[1] Campus Computing survey for 2006 (http://www.campuscomputing.net/) reports that over 80 percent of respondents have policies related to downloading music and videos. EDUCAUSE "Core Data Service" survey (*http://www.educause.edu/coredata/*) shows that nearly 95 percent of respondents shape or track bandwidth utilization. The 2006 RESNET survey (*http://www.resnetsymposium.org/surveys/2006securitysurvey.htm*) indicates that roughly 80 percent of respondents "block, filter, or otherwise restrict" P2P traffic between residence halls and the Internet.

software use and developing a curriculum component to combat illegal downloads, working with industry leaders to create educational fair use media definitions and faster copyright use, providing rewards for our students.[2]

Dean Cheryl Elzy will testify further about the project.

Issues

Are products currently available that meet the requirements of campus network environments?

No single, silver-bullet, solution is available to stop unauthorized distribution of digital media while allowing authorized traffic. The variety of campus network needs and policies with respect to the proper role of the institution in policing users leads to a highly heterogeneous environment for vendors. However, recent work by the Joint Committee has helped build an understanding of these varied requirements and given technology companies insight into how their products might better meet campus needs. In addition, many mature products are available that can contribute in part to a holistic anti-piracy solution. Many campuses already use some type of filtering tools in all or part of there network. In addition, the availability of legitimate alternatives for entertainment content and secure methods for transferring teaching material has grown significantly in recent years.

Does peer-to-peer (P2P) software have non-infringing use?

It is clear that a great deal of P2P traffic involves copyrighted content; however significant, legal uses of the technology are also available. Some examples include: BitTorrent, a general file-transfer protocol that has been implemented for legal downloads of software and movies, Skype, an Internet telephony program, and Vudu, producer of a tv set-top box providing movie screenings via P2P downloads. Therefore, many campuses are reluctant to censor all P2P traffic and prefer solutions that try to identify specific infringing activity. Due to the complexity of the copyright system, however, differentiating infringing use from allowed use remains technologically difficult. The witnesses will be able to discuss what options are available that block piracy while allowing the transfer of educational materials.

What role should education about copyright play and at what level?

Many colleges and universities report undertaking some kind of education campaign, particularly geared towards incoming freshmen classes. Education techniques may range from simple notifications of campus policy on copyright infringement to short video segments defining student's rights and responsibilities or ongoing awareness campaigns. Many colleges and universities contend that piracy is established as a social norm before students enter collegiate study, and that education on what is and is not allowed under copyright law should begin in a K–12 setting. One goal of the Digital Citizens Project will be to systematically study education campaigns for their effectiveness.

What can campus efforts to combat piracy tell us about broader piracy controls?

Campus networks comprise just part of the larger piracy problem. Commercial providers of Internet service have also seen growing complaints from copyright holders and many colleges contend that piracy begins well before students arrive on campus. Commercial networks could implement similar controls, and would face similar social and technological challenges, to those used by colleges and universities.

What rights do higher education institutions have to use copyrighted material?

Under the Copyright Act, teachers are exempt from infringement for performing copyrighted works in certain educational contexts. Performance of a work done in the course of face-to-face instruction in a classroom, or performances done as part of instructional activities of a nonprofit institution, may not be an infringement of copyright.[3]

What rights do users have to use copyrighted material?

Although most uses of copyrighted materials require permission from the copyright holder, the *Copyright Act of 1976* provides several exceptions for the use of

[2] Digital Citizen Project. *http://www.digitalcitizen.ilstu.edu/summary/*

[3] Yeh, B.T. Congressional Research Service. RL33631—Copyright Licensing in Music Distribution, Reproduction, and Public Performance.

copyrighted material, regardless of the holder's permission. The doctrine of "fair use" recognizes the right of the public to make reasonable use of copyrighted material, in special instances, without the copyright holder's consent. Because the language of the fair use statute is illustrative, determinations of fair use are often difficult to make in advance. However, the statute recognizes fair use "for purposes such as criticism, comment, news reporting, teaching, scholarship, or research." A determination of fair use considers four factors:

* The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes.
* The nature of the copyrighted work.
* The amount and substantiality of the portion used in relation to the copyrighted work as a whole.
* The effect of the use upon the potential market for/or value of the copyrighted work.

The U.S. Supreme Court has previously explained that this four-factor test cannot be simplified by "bright-line rules," but rather that the doctrine of fair use calls for "case-by-case" analysis. In the context of digital music downloads and transmissions, some alleged copyright infringers have attempted to use the doctrine of fair use to avoid liability for activities such as sampling, "space shifting," and peer-to-peer filesharing. These attempts have not been very successful: several federal appellate courts have ruled against the applicability of the fair use doctrine for these purposes. The difficulty behind any fair use determination, however, is the irresolute nature of the exception—one court's determination of fair use may be another's determination of infringement.[4]

[4] Yeh, B.T. Congressional Research Service. RL33631—Copyright Licensing in Music Distribution, Reproduction, and Public Performance.

Copyright Violation Notifications Sent to Colleges and Universities

MPAA list	RIAA list
1,198 Columbia University	University of Wisconsin system (66, including the following individual campuses: Eau Claire, Madison, Milwaukee, Parkside, Platteville, Stevens Point, Stout, and Whitewater),
934 University of Pennsylvania	Boston University (50)
891 Boston University	Purdue University (38)
889 University of California at Los Angeles	University of Maine system (27)
873 Purdue University	University of Nebraska - Lincoln (25)
860 Vanderbilt University	University of California - Los Angeles (21)
813 Duke University	Columbia University (20)
792 Rochester Institute of Technology	Drexel University (20)
765 University of Massachusetts	Ithaca College (20)
740 University of Michigan	Vanderbilt University (20)
714 University of California at Santa Cruz	University of California - Berkeley (19),
704 University of Southern California	DePaul University (18)
637 University of Nebraska at Lincoln	Ferris State University (17)
636 North Carolina State University	University of California - Santa Cruz (17)
586 Iowa State University	Virginia Polytechnic Institute & State University (16)
575 University of Chicago	Dartmouth College (11)
562 University of Rochester	
550 Ohio University	
527 University of Tennessee	
506 Michigan State University	
457 Virginia Polytechnic Institute	
455 Drexel University	
447 University of South Florida	
405 Stanford University	
398 University of California at Berkeley	

Higher Education Actions to Address Illegal Campus Peer-to-Peer Filesharing

History and Past Activities

- Formation of the *Joint Committee of the Higher Education and Entertainment Communities:* The higher education community joined with the entertainment industry to form the Joint Committee, operating through the support and guidance of the American Council on Education (ACE), the Association of American Universities (AAU), EDUCAUSE, the Recording Industry Association of America (RIAA), and the Motion Picture Association of America (MPAA) *[December, 2002]*
- Work of higher education through the Joint Committee
  - Distribution to colleges and universities of *Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P Filesharing on University Networks [August, 2003]*
  - Joint Committee-sponsored meeting of higher education and entertainment association officials, representatives of entertainment companies and online digital delivery services to discuss how these sectors can collaborate to reduce illegal and promote legal P2P *[June, 2003]*
  - Report to colleges and universities of results of Request for Information on technologies that may assist in reducing unauthorized P2P filesharing *[October, 2003]*

- Report to colleges and universities on legitimate online digital content delivery services that might be engaged as alternatives to unauthorized P2P filesharing programs *[December, 2003]*
- Distribution of *University Policies and Practices Addressing Improper Peer-to-Peer Filesharing [April, 2004]*
- Collaboration with RIAA to produce and distribute a video on P2P intended for college freshmen orientation *[spring–summer, 2006]*
- Meeting of university, entertainment industry, and technology vendor officials to examine network technologies to reduce illegal P2P filesharing *[October, 2006]*
- Distribution of updated paper on legal aspects of campus P2P, *Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P Filesharing on University Networks [November, 2006]*
- Joint Committee meeting to assess past work, current challenges, and future steps *[November, 2006]*

- Numerous presentations at higher education association meetings, written communications to colleges and universities, about illegal campus P2P filesharing and reference to resources to address the problem *[Ongoing]*

Current and Projected Activities

- Formed new Technology Task Force to work with commercial vendors to facilitate development of effective technologies to reduce campus P2P
- Formed campus officials group to work with RIAA to revise video for freshman orientation and promote broad adoption by campuses
- Letter from ACE President David Ward to college and university presidents and chancellors transmitting an RIAA letter announcing a new round of lawsuits accompanied by a "pre-notice plan" that allows settlement of claims before filing of a lawsuit
- Conduct survey of colleges and universities to identify effective policies and practices for reducing illegal P2P filesharing, develop updated best practices recommendations for distribution to colleges and universities
- Continue to discuss P2P activities and share information through national meetings and written communications