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

HEARING CHARTER

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 file sharing in the U.S. cost the movie industry $500 million, an estimated 44% 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 campuses 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 US 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 National 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 email 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% 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% 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.