

May 2004

FILE SHARING

Selected Universities Report Taking Action to Reduce Copyright Infringement



G A O

Accountability * Integrity * Reliability

Highlights of [GAO-04-503](#), a report to congressional requesters

Why GAO Did This Study

The emergence of peer-to-peer file-sharing applications that allow networks to share computer files among millions of users has changed the way copyrighted materials, including digital music, videos, software, and images can be distributed and has led to a dramatic increase in the incidence of copyright infringement (piracy) of these digital materials. These applications enable direct communication between users, allowing users to access each other's files and share digital music, videos, and software. According to a coalition of intellectual property owners in the entertainment industry, an increasing number of students are using the fast Internet connections offered by college and university networks to infringe copyrights by illegally downloading and sharing massive volumes of copyrighted materials on peer-to-peer networks.

GAO was asked to describe (1) the views of major universities on the extent of problems experienced with student use of file-sharing applications as well as the actions that the universities are taking to deal with them and (2) the actions that federal enforcement agencies have taken to address the issue of copyright infringement on peer-to-peer networks as well as agency views on any legislative barriers to dealing with the problems.

www.gao.gov/cgi-bin/getrpt?GAO-04-503.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzlj@gao.gov.

FILE SHARING

Selected Universities Report Taking Action to Reduce Copyright Infringement

What GAO Found

The college and university officials we interviewed are aware of the use of file-sharing applications on their networks, almost all of them have experienced some problems and increased costs as a result of the use of these applications, and they are taking steps to reduce the use of these applications on their networks. All of the officials interviewed indicated that their colleges or universities routinely monitor their networks, and most of them indicated that the institutions also actively monitor their networks specifically for the use of these file-sharing applications. When infringing use is discovered, all of the representatives stated that enforcement actions are taken against the individuals responsible. These actions included issuing a warning to the user or users, banning them from the network for a period of time, and managing the bandwidth available for a group of users.

Federal law enforcement officials have been taking action to investigate and prosecute organizations involved in significant copyright infringement. These groups use a wide range of Internet technologies to illegally distribute copyrighted materials over the Internet. Federal law enforcement officials did not identify any specific legislative barriers to investigation and prosecution of illegal file sharing on peer-to-peer networks. According to the Department of Justice officials, the department's recently created Intellectual Property Task Force will examine how the department handles intellectual property issues and recommend legislative changes, if needed.

U.S. Customs Agent with Hard Drives Seized during Operation Buccaneer



Source: U.S. Immigration and Customs Enforcement.

Contents

Letter		1
	Results in Brief	2
	Background	4
	Selected Universities Report Taking Action to Reduce Illegal File Sharing on Campus Networks	8
	Federal Enforcement of Copyright Infringement through File Sharing Focuses on Organized Groups	15
	Summary	19
	Agency Comments and Our Evaluation	20
Appendix I	Objectives, Scope, and Methodology	22
Appendix II	Description of File Sharing and Peer-to-Peer Networks	24
Appendix III	Key and Supporting Federal Agencies Involved in the Investigation and Prosecution of Copyright Infringement	30
	Investigating Agencies	30
	Prosecuting Agencies	31
	Supporting Agencies	32
Appendix IV	Comments from the Department of Justice	34
Glossary		38
Table		
	Table 1: Federal Entities and Supporting Agencies and Organizations Involved in the Investigation and Prosecution of Intellectual Property Rights Violations and Copyright Infringement	7

Figures

Figure 1: Average Percentage of Bandwidth Used for Peer-to-Peer File Sharing (Selected universities)	9
Figure 2: Number of Notifications and Ability to Trace to an Individual Student (Selected universities)	10
Figure 3: Expenses Associated with Responding to Peer-to-Peer File Sharing: Amount of Reported Additional Funding and Categories of Expense (Selected universities)	11
Figure 4: Educational Activities: Planned and Completed (Selected universities)	13
Figure 5: Enforcement Activities Used (Selected universities)	14
Figure 6: U.S. Customs Agent with Hard Drives Seized during Operation Buccaneer	17
Figure 7: Peer-to-Peer Models	26
Figure 8: Topology of a Gnutella Network	29

Abbreviations

CIO	chief information officer
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
IM	Instant messaging
IP	Internet Protocol
VNS	virtual name space

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



G A O

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 28, 2004

The Honorable Ted Stevens
Chairman, Committee on Appropriations
United States Senate

The Honorable Harry Reid
Assistant Minority Leader
United States Senate

The Honorable John A. Boehner
Chairman, Committee on Education and the Workforce
House of Representatives

The Honorable Howard P. McKeon
Chairman, Subcommittee on 21st Century Competitiveness
Committee on Education and the Workforce
House of Representatives

File sharing—the use of peer-to-peer¹ networks to distribute computer files among millions of users—has dramatically changed the way copyrighted materials, including digital music, videos, software, and images can be distributed. By permitting fast, cheap, and easy production of identical copies, file-sharing applications have facilitated both the legitimate distribution of copyrighted materials by the copyright holder and the illegal copyright infringement (piracy) and distribution by unauthorized users. According to a coalition of intellectual property owners in the recording industry, an increasing number of students are using fast Internet connections offered by college and university networks to infringe copyrights by illegally downloading and sharing massive volumes of copyrighted songs, movies, and video games on peer-to-peer networks.

As requested, our objectives were to describe (1) the views of major universities on the extent of problems experienced with student use of

¹Peer-to-peer file-sharing network programs enable direct communication between users, allowing them to access each other's files and share digital music, software, images, and videos.

file-sharing software applications, as well as the actions that the universities are taking to deal with them and (2) the actions that federal enforcement agencies have taken to address the issue of copyright infringement on peer-to-peer networks, as well as agency views on any legislative barriers to dealing with the problems.

To address the first objective, we conducted structured interviews with a judgmentally selected group of 13 officials that oversee the computer systems of major postsecondary educational institutions. The selected colleges and universities were located in each of eight geographic regions of the United States. All of these institutions provided Internet access to students in university-administered housing and were large public or private degree-granting colleges and universities. In this analysis, we provide details on the responses of the 13 college or university officials we interviewed; however, because we did not randomly select interviewees, our results are not generalizable to all colleges or universities.

To describe federal law enforcement efforts and agency views related to copyright infringement on peer-to-peer networks, we analyzed budget and program documents from the Department of Justice (Justice) Computer Crime and Intellectual Property Section; the Federal Bureau of Investigation (FBI) Cyber Division; and the Cyber Crimes Center of the Bureau of Immigration and Customs Enforcement, Department of Homeland Security (DHS). We also interviewed officials from these organizations.

We performed our work from May 2003 to April 2004 in accordance with generally accepted government auditing standards. Further details on our objectives, scope, and methodology are provided in appendix I.

Results in Brief

The college and university officials we interviewed are aware of the use of file-sharing software applications on their networks; and almost all of them report that they have experienced some problems and increased costs as a result of the use of these applications, therefore, they are taking steps to reduce the use of peer-to-peer file-sharing technology on their networks. Specifically, several of the college or university officials interviewed stated that, on average, a significant amount of bandwidth on their networks appeared to be used for file-sharing applications; several of the respondents estimated that a sizable portion of the students at the college or university were using file-sharing applications to download or share music, images, and video files during the 2003 to 2004 academic term. Further, most of the officials interviewed stated that their

institutions had experienced either network performance problems or security incidents as a result of the use of the file-sharing applications on their networks, and almost all indicated that they had spent additional funds to deal with the problems associated with the use of these applications, including two respondents who indicated that they had spent between \$250,000 and \$749,999.

At the same time, all the college and university officials we interviewed stated that they have implemented technical controls to limit the use of file-sharing technology on their networks and that they have either undertaken or plan to undertake educational and enforcement efforts to limit student copyright infringement. Further, most of the officials interviewed stated that they felt they had the right tools and knowledge to address the issue and that they thought the approaches they have used have been either somewhat or very successful at controlling the problem.

Federal law enforcement officials are taking actions to investigate and prosecute organized software-piracy groups that use a wide range of Internet technologies—including file sharing over peer-to-peer networks—to illegally distribute copyrighted materials over the Internet. Two recent examples of major federal law enforcement action that has focused on international piracy groups are (1) the Operation Fastlink coordinated by Justice Computer Crime and Intellectual Property Section and the Federal Bureau of Investigation, and (2) Operation Buccaneer, led by the U.S. Customs Service and Justice. These operations resulted in the identification of individuals engaged in online piracy and the seizure of tens of thousands of pirated copies of software, music, and computer games worth millions of dollars.

Federal law enforcement officials did not identify any specific legislative barriers to investigation and prosecution of illegal file sharing on peer-to-peer networks. According to Justice officials, the department's recently created Intellectual Property Task Force will examine how the department handles intellectual property issues and recommend legislative changes, assuming there is a need for such changes.

In commenting on a draft of this report, the Deputy Assistant Attorney General provided information on a recent international law enforcement effort against online piracy and presented additional detail on the department's policy on investigating and prosecuting intellectual property rights infringers on the Internet and on the peer-to-peer networks. These comments, which are reprinted in appendix IV, have been incorporated into this report as appropriate.

In addition, we received comments (via e-mail) from the unit chief of the Cyber Crime Center on behalf of DHS. The unit chief clarified the center's approach to investigations of individual copyright infringers and provided various technical comments, which have been incorporated into this report as appropriate.

Background

U.S. copyright law protects books, photographs, videos, movies, sound recordings, software code, and other creative works of expression from unauthorized copying. A copyright gives its owner the exclusive right to reproduce, distribute, perform, display, or license a work, and the exclusive right to produce or license the production of derivative works.² Copyright protection attaches as soon as the work is "fixed in a tangible medium of expression," thus covering both published and unpublished works. However, there are some limits to the protections afforded by copyright law, such as in the use of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, scholarship, or research.³

File Sharing Is a Principal Tool for Distribution of Copyrighted Works

File-sharing software applications work by making selected files on a user's computer available for downloading by anyone using similar software, which, in turn, gives the user access to selected files on computers of other users on the peer-to-peer network. The growing popularity and proliferation of file-sharing applications such as KaZaA has had a profound effect on the dissemination of copyrighted works, by both the copyright holder and infringers.

The use of file sharing has grown steadily over the past few years. For example, by May 2003, KaZaA had become the world's most downloaded software program of any kind, with more than 230 million⁴ downloads. According to the Recording Industry Association of America, the

²17 U.S.C. §§ 106, 201(d).

³For example, a copyright holder's exclusive right to distribute and perform the work, make reproductions, and create derivative works is limited by the fair-use doctrine. The fair-use doctrine operates as a limitation on and exception to the rights granted by copyright by permitting the copying of copyrighted works for certain uses that include criticism, commentary, news reporting, teaching, scholarship, or research. Use of copyrighted work is not an infringement if the use falls within the scope of "fair use," based on a case-by-case analysis of four factors identified by statute.

⁴Testimony of Cary Sherman, President, Recording Industry Association of America before Senate Committee on Commerce, Science, and Transportation, September 17, 2003.

increased use of peer-to-peer networks has contributed to an increase in copyright infringement, with millions of users downloading more than 2.6 billion copyrighted files (mostly sound recordings) each month via various peer-to-peer networks.

The widespread unauthorized distribution of copyrighted material on peer-to-peer systems is a concern not only for copyright owners but also for those who administer the networks on which the file-sharing applications run. Because of their high-bandwidth connections and the concentration of large groups of young, computer-literate users, college and university networks are particularly vulnerable to adverse impacts from the use of file-sharing applications. In 2002, a committee of representatives from education and the entertainment industry—the Joint Committee of Higher Education and Entertainment Communities—was convened to discuss and address matters of mutual concern, including the misuse of university networks for copyright infringement. In addition, the Recording Industry Association of America has conducted searches for copyrighted material being illegally shared on peer-to-peer networks and has sent more than 30,000 notices to colleges and universities regarding files that are being shared on systems connected to university networks.

Congress has moved to address piracy issues that have been raised by developments in computer and Internet technology. With regard to the widespread unauthorized distribution of copyrighted material on peer-to-peer systems, the crime of felony copyright infringement has four essential elements:

1. A copyright exists;
2. The copyright was infringed by the defendant, specifically by reproduction or distribution of the copyrighted work, including by electronic means;
3. The defendant acted “willfully.” Under the law, evidence of reproduction or distribution of a copyrighted work, by itself, is not sufficient to establish willful infringement; and

-
4. The defendant infringed at least 10 copies of one or more copyrighted works with a total retail value of more than \$2,500 within a 180-day period.⁵

In addition to criminal liability, significant civil remedies are available to copyright holders for infringement. Copyright holders are entitled to receive either “actual damages and profits” from an infringer, or they can elect to receive “statutory damages” ranging from \$750 to \$30,000 for each infringed work, increasing to \$150,000 if the copyright holder proves the infringement was willful. In addition, a court can order an injunction against further infringement, the impoundment and disposition of infringing articles, and attorneys’ fees and costs.⁶

Federal Agencies Have Law Enforcement Responsibilities Regarding Illegal File Sharing

Several federal entities are responsible for enforcing the federal statutes pertaining to intellectual property protection and copyright infringement. Table 1 shows these agencies, along with other key organizations involved in efforts to protect intellectual property rights and combat copyright infringement, including illegal file sharing on peer-to-peer networks.

⁵Generally, the criminal infringement statute provides that where the offense consists of willful infringement of a copyright with a retail value of at least \$2,500 over a 180-day period, the penalty is not more than 5 years imprisonment if the offense was for the purpose of commercial advantage or private financial gain, that is, there is an attempt to gain an advantage or profit (violations of 17 U.S.C. § 506(a)(1)). If the infringement consists of willful distribution and reproduction of copyrighted materials with no aspect of commercial advantage or private financial gain (violations of 17 U.S.C. § 506(a)(2)), the penalty is not more than 3 years imprisonment.

⁶17 U.S.C. § 502-505.

Table 1: Federal Entities and Supporting Agencies and Organizations Involved in the Investigation and Prosecution of Intellectual Property Rights Violations and Copyright Infringement

Agency	Unit	Focus
Investigating agencies		
Department of Homeland Security	Cyber Crimes Center, U.S. Immigration and Customs Enforcement	Investigates international criminal activity conducted on or facilitated by the Internet, including money laundering, drug trafficking, intellectual property rights violations, arms trafficking, and child pornography, and provides computer forensics support to other agencies.
Department of Justice	Cyber Division, Federal Bureau of Investigation	Investigates federal violations, including intellectual property rights violations, in which the Internet, computer systems, and networks are exploited as the principal instruments or targets of criminal activity.
Prosecuting agencies		
Department of Justice	Computer Crime and Intellectual Property section	Consists of specialized attorneys who prosecute cybercrime and intellectual property cases worldwide.
	Computer Hacking and Intellectual Property units	Consist of prosecutors in select U.S. Attorneys Offices dedicated primarily to prosecuting high-technology crimes, including intellectual property offenses.
	Computer and Telecommunication Coordinator network	Consists of prosecutors in U.S. Attorneys Offices specifically trained to address the range of novel and complex legal issues related to high-tech and intellectual property crime.
	U.S. Attorneys Offices	Serve as the nation's principal litigators under the direction of the U.S. Attorney General.
Supporting agencies		
Department of Commerce	International Trade Administration	Monitors foreign governments' compliance and implementation of international trade agreements, especially those pertaining to intellectual property rights enforcement.
Department of Homeland Security	Intellectual Property Rights Coordination Center, U.S. Immigration and Customs Enforcement	Coordinates the investigation of leads provided by the general public and industry pertaining to intellectual property rights infringement. The Center is a joint effort of the Immigration and Customs Enforcement and the Federal Bureau of Investigations.
Department of Justice	Criminal Division	Provides, through its Overseas Prosecutorial Development, Assistance and Training Office and its International Criminal Investigation Training Assistance Programs, training and assistance to foreign law enforcement and foreign governments to foster the robust protection of intellectual property rights in foreign countries.
	Federal Bureau of Investigation	Fosters the protection of intellectual property rights in foreign countries and assists U.S. prosecutions of intellectual property violations originating in foreign countries through its legal attaches located in foreign countries.
Department of State	International Law Enforcement Academies	Provides specialized training courses in fighting intellectual property rights crime.
National Intellectual Property Law Enforcement Coordination Council	Interagency Coordination Council	Coordinates domestic and international intellectual property law enforcement among federal and foreign entities (including law enforcement liaison, training coordination, industry and other outreach) and increases public awareness.

Source: GAO analysis of agency data.

The federal law enforcement agencies work with state and local law enforcement agencies, including state police and local district attorneys, in the investigation and prosecution of intellectual property crime. In addition, industry organizations, such as the Recording Industry Association of America, the Business Software Alliance, and the Software and Information Industry Association, provide federal law enforcement organizations with information and documentary evidence in support of federal investigations and prosecutions. (See app. III for a detailed description of federal organizations involved in investigating and prosecuting copyright infringement.)

Selected Universities Report Taking Action to Reduce Illegal File Sharing on Campus Networks

The college and university officials we interviewed are aware of the use of file-sharing applications on their networks, almost all of them have experienced some problems and increased costs as a result of the use of these applications, and they are taking steps to reduce the use of peer-to-peer file-sharing technology on their networks.⁷

All of the college and university officials we interviewed stated that they have implemented technical controls to limit the use of file-sharing technology on their networks and that they have either undertaken or plan to undertake educational and enforcement efforts to limit student copyright infringement. Most of the officials interviewed stated that they felt they had the right tools and knowledge to deal with the use of peer-to-peer file-sharing applications to download or share copyrighted material on university networks, and almost all of the officials stated that they thought the approaches they have used to address the problem have been either somewhat or very successful at controlling the problem.

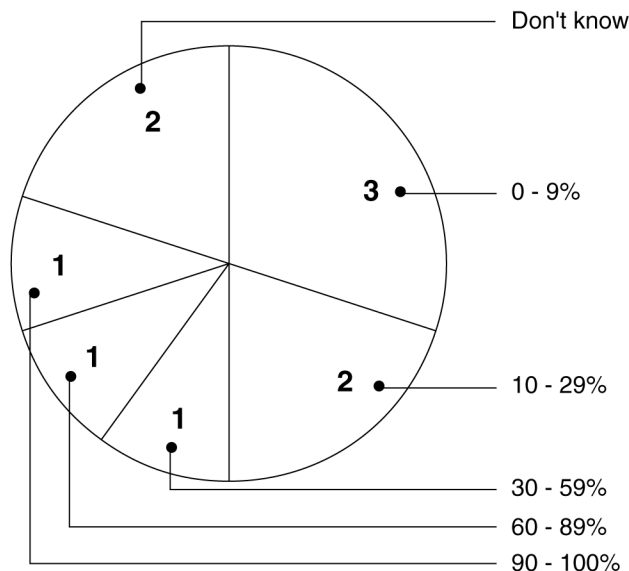
University Officials We Interviewed Are Aware of the Use of File-Sharing Applications on Their Networks

All of the university officials we interviewed indicated that their colleges or universities routinely monitor their networks and most of them indicated that the institutions also actively monitored their networks specifically for the use of peer-to-peer file-sharing applications during the 2003 to 2004 academic term. For those colleges and universities that monitored specifically for the use of file-sharing technology (10 of 13 respondents), university officials stated that the amount of bandwidth that

⁷Although we provide details on the responses of the 13 college or university officials we interviewed, our results are not generalizable to all colleges or universities.

appeared to be used by file-sharing applications varied, from as low as 0 to 9 percent to as high as 90 to 100 percent. (See fig. 1.)

Figure 1: Average Percentage of Bandwidth Used for Peer-to-Peer File Sharing (Selected universities)

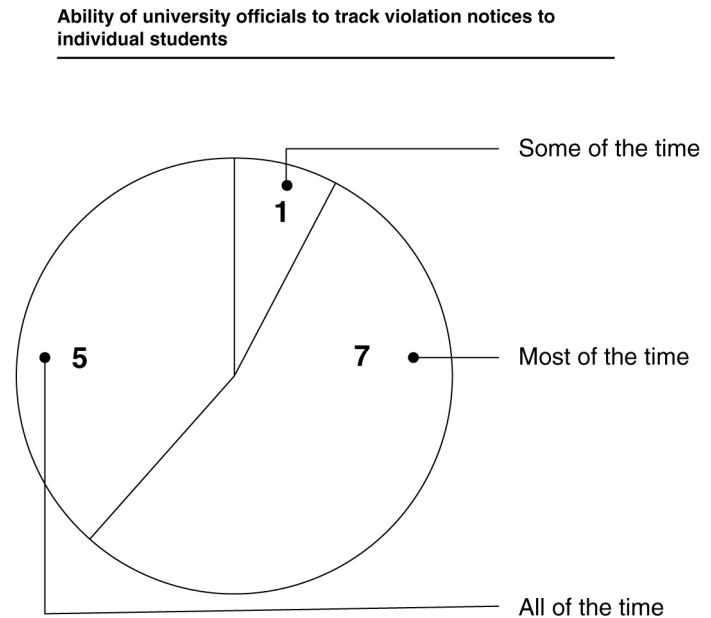
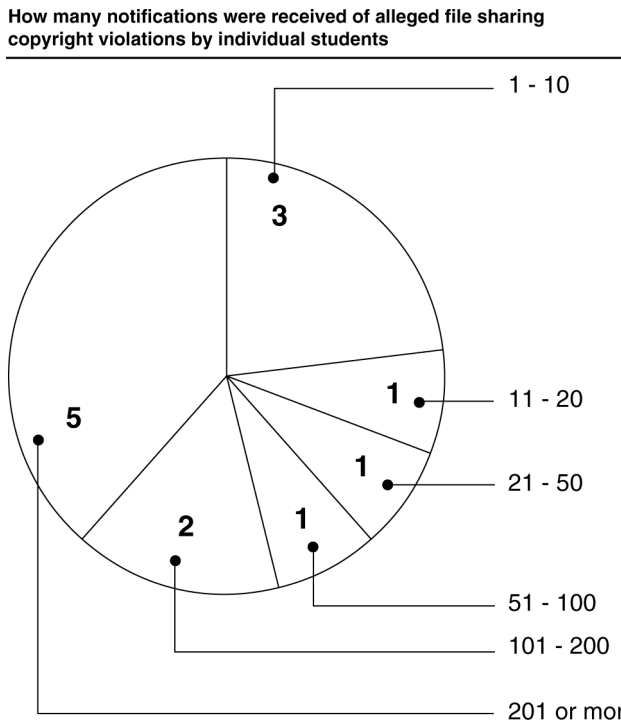


Source: GAO analysis of survey responses.

While several university officials were unable to estimate the percentage of students using file-sharing applications to download or share music, images and video files, several estimated that 30 percent or more of students were doing so during the 2003 to 2004 academic term. One official estimated that between 90 and 100 percent of the students at the institution were using file-sharing applications.

In addition, all of the college and university officials interviewed indicated that they had received notices from representatives of copyright holders alleging file-sharing copyright violations by students, with more than half of the interview respondents indicating that they had received more than 100 notifications. In most or all of these cases, university officials were able to trace the infringement notification to an individual student. (See fig. 3.)

Figure 2: Number of Notifications and Ability to Trace to an Individual Student (Selected universities)



Source: GAO analysis of survey responses.

Use of Peer-to-Peer Technology Has Reportedly Had a Negative Impact on University Networks

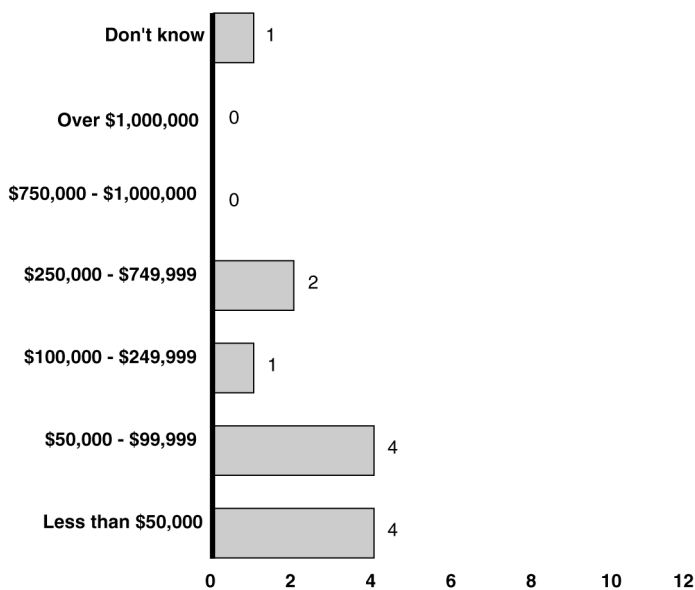
Overall, most of the college and university officials we interviewed indicated that they had experienced some network performance or security problems as a result of the use of peer-to-peer file-sharing applications on their institutions' networks. Specifically, two officials interviewed stated that their institution had experienced network performance problems somewhat often as a result of student use of file-sharing applications, and six officials indicated that they had experienced few network performance problems. Further, of the 13 institutions whose officials we interviewed, 9 indicated that they had experienced security problems as a result of file sharing or downloading. For those who indicated that they had experience problems, the most common types of security incidents reported were the introduction of viruses or malicious code (eight interview respondents) and temporary loss of network resources (five interview respondents).

In addition, almost all of the officials that were interviewed stated that their institutions had spent additional funding during the 2003 to 2004

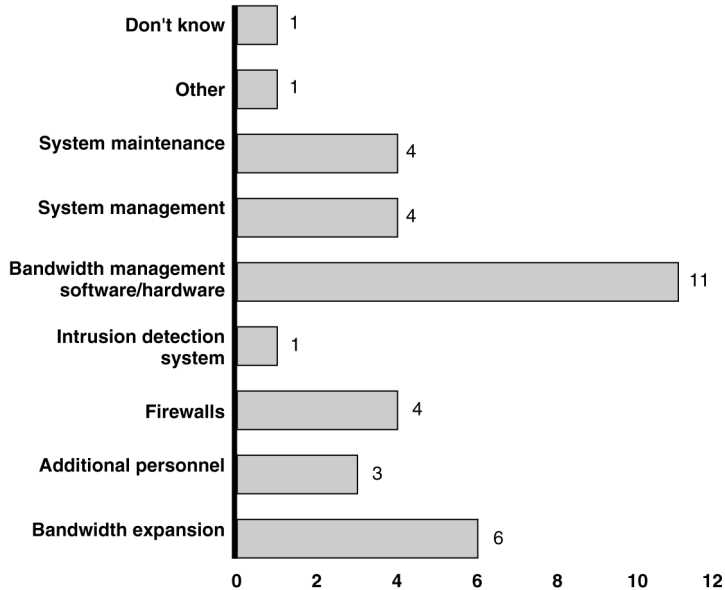
academic year to deal with the effects of the use of peer-to-peer file-sharing applications on their networks, with the median amount of additional spending being between \$50,000 and \$99,999;⁸ two officials stated that their institutions had spent between \$250,000 to \$749,999. This additional funding was spent on a variety of network infrastructure and operational areas, including bandwidth expansion, bandwidth management software/hardware, system management, and system maintenance. (See fig. 3.)

Figure 3: Expenses Associated with Responding to Peer-to-Peer File Sharing: Amount of Reported Additional Funding and Categories of Expense (Selected universities)

Additional funding spent by your institution for network infrastructure and operations



On which of the following items, if any, did you spend the additional funds?



Source: GAO analysis of survey responses.

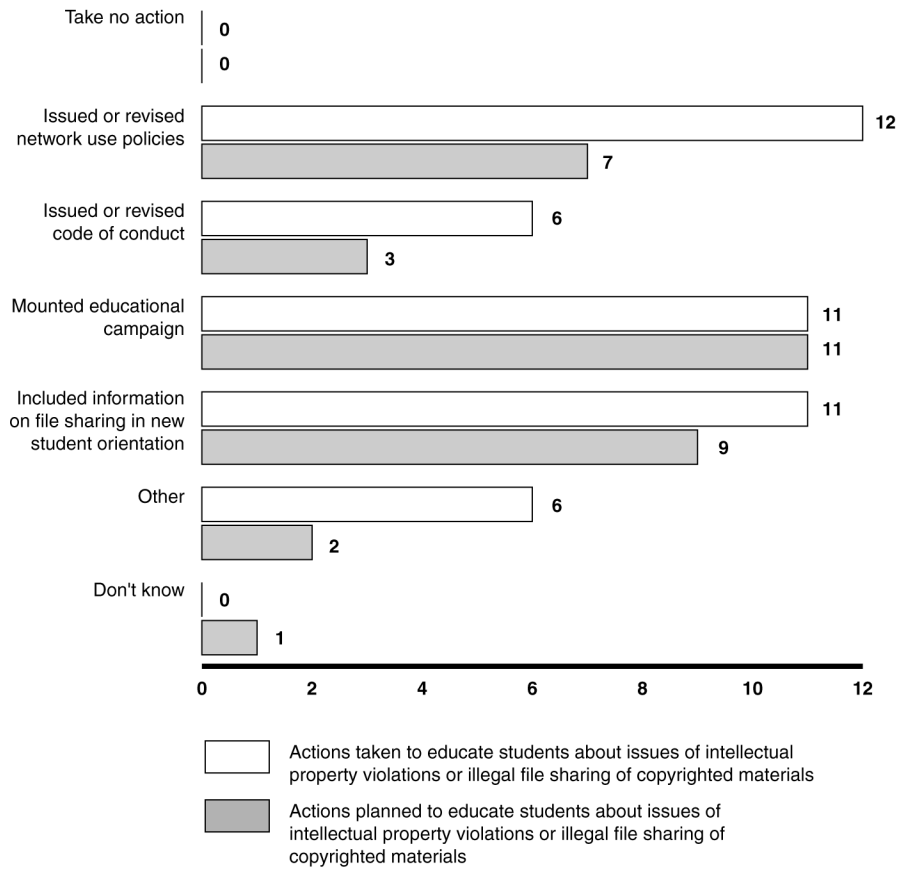
⁸A median is the value in an ordered set of values below and above which there is an equal number of values; if there is no one middle number, it is the value that is the arithmetic mean of the two middle values.

Universities Report Taking Steps to Reduce Copyright Infringement on Peer-to-Peer Networks

All of the colleges and universities whose officials we interviewed indicated that they are taking steps to reduce or eliminate the use of peer-to-peer file-sharing technology for copyright infringement on their networks. Specifically, all of the officials interviewed stated that they have implemented technical controls to limit the use of file-sharing technology. These technical controls include (1) limiting access to file-sharing applications, both among internal users of the network and between internal and external users; (2) reducing or limiting the amount of bandwidth available to network users seeking to download or share files; and (3) segregating the portion of the network serving college or university administered housing from the rest of the university network.

In addition, all of the officials interviewed stated that they have either undertaken or plan to undertake educational and enforcement efforts to limit student copyright infringement. All of the officials that were interviewed stated that they have undertaken educational efforts, such as issuing or revising network use policies and student codes of conduct; and 12 of the 13 officials that were interviewed stated that they plan to undertake educational activities regarding intellectual property violations or illegal file sharing of copyrighted materials. (See fig. 4.)

Figure 4: Educational Activities: Planned and Completed (Selected universities)



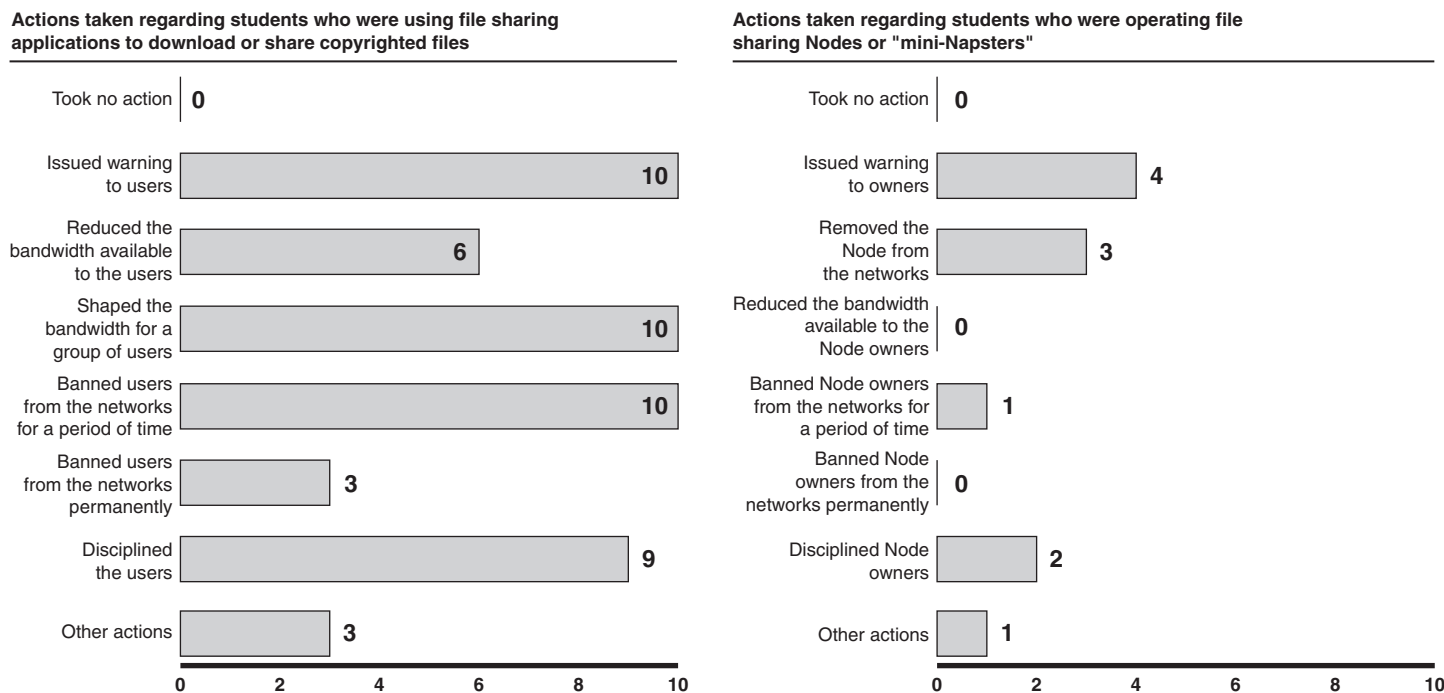
Source: GAO analysis of survey responses.

Further, all the officials interviewed stated that they have undertaken enforcement efforts to address copyright infringement on peer-to-peer networks. During the 2002 to 2003 academic year, all of the college and university officials interviewed stated that they had either discovered or had been made aware of individuals using file-sharing applications such as KaZaA or peer-to-peer network indexes⁹ on their institution's network. When file downloading was discovered, all the officials stated that

⁹Peer-to-peer network indexes are high-capacity searchable indexes of files located on other computers on a local area network (similar to the original Napster; see app. II). These indexes are sometimes also referred to as "mini-Napsters" and use software such as *Phynd* to create and maintain searchable indexes of files shared on a peer-to-peer network.

enforcement actions were taken against the individuals responsible. These actions included issuing a warning to the user or users, banning them from the network for a period of time, and shaping the bandwidth available for a group of users. (See fig. 5.)

Figure 5: Enforcement Activities Used (Selected universities)



Source: GAO analysis of survey responses.

Most of the officials interviewed stated that they felt they had the right tools and knowledge to deal with the use of peer-to-peer file-sharing applications to download or share copyrighted material. Further, almost all of the officials stated that they thought the approaches they have used to address the problem have been either somewhat or very successful at controlling the use of peer-to-peer applications for downloading and sharing copyrighted materials.

Federal Enforcement of Copyright Infringement through File Sharing Focuses on Organized Groups

Federal law enforcement officials told us that they have been taking actions to investigate and prosecute organizations involved in significant copyright infringement, such as the warez¹⁰ groups—loosely affiliated networks of criminal groups that specialize in “cracking” the copyright protection on software, movies, game and music files. These groups use a wide range of Internet technologies—including file sharing over peer-to-peer networks—to illegally distribute copyrighted materials over the Internet. According to the Deputy Chief for Intellectual Property Computer Crime and Intellectual Property Section, Justice, the top warez groups serve as major suppliers of the infringed works that eventually enter the stream of file sharing on peer-to-peer networks.

Two recent examples of major federal law enforcement actions that have focused on international piracy groups are the Justice’s Operations Fastlink and the U.S. Customs Service’s Operation Buccaneer.

Operation Fastlink is an international investigation coordinated by Justice’s Computer Crime and Intellectual Property Section and the FBI. According to the Deputy Chief for Intellectual Property Computer Crime and Intellectual Property Section, Fastlink is the largest international enforcement effort ever undertaken against online piracy. As part of Operation Fastlink, on April 21, 2004, U.S. and foreign law enforcement officials executed more than 120 simultaneous searches across multiple time zones. In addition to the United States, searches were executed in Belgium, Denmark, France, Germany, Hungary, Israel, the Netherlands, Singapore, Sweden, Great Britain, and Northern Ireland. As a result, more than 100 individuals believed to be engaged in online piracy have been identified, many of them high-level members or leaders of online piracy release groups that specialize in distributing high-quality pirated movies, music, games, and software over the Internet. More than 200 computers were seized worldwide, including more than 30 computer servers that function as storage and distribution hubs for the online piracy groups targeted by this operation.

Operation Buccaneer was an international investigation and prosecution operation led by the U.S. Customs Service and Justice. The operation resulted in the seizure of tens of thousands of pirated copies of software,

¹⁰Warez refers to software applications that have had all copy protection removed or circumvented, and are therefore available for unlimited copying, free of charge, in violation of the software owner’s or publisher’s copyright.

music, and computer games worth millions of dollars and led to 30 convictions worldwide. Operation Buccaneer targeted a number of highly organized and sophisticated international criminal piracy groups that had cracked the copyright protection on thousands of software, movie, and music files and distributed those files over the Internet.

As part of Operation Buccaneer, on December 11, 2001, the U.S. Customs Service and law enforcement officials from Australia, Finland, Norway, Sweden, and the United Kingdom simultaneously executed approximately 70 search warrants worldwide. Approximately 40 search warrants were executed in 27 cities across the United States, including several at universities. Pursuant to the search warrants, law enforcement seized 10 computer “archive sites” that contained tens of thousands of pirated copies of software, movies, music, and computer games worth millions of dollars. According to the Deputy Chief for Intellectual Property Computer Crime and Intellectual Property Section, as of April 1, 2004, 27 defendants had been convicted in the United States, with 2 awaiting sentencing and 1 other under indictment. Internationally, six defendants have been convicted in Finland and the United Kingdom, with four additional defendants scheduled to go to trial in the United Kingdom in the fall of 2004.

Figure 6: U.S. Customs Agent with Hard Drives Seized during Operation Buccaneer



Source: U.S. Immigration and Customs Enforcement.

According to DHS officials, the Cyber Crime Center of the U.S. Immigration and Customs Enforcement does target individual violators who are involved in cyber intellectual property piracy on a profit or commercial basis. The officials noted that the center does not pursue investigations of individual peer-to-peer file violators due to the statutory dollar-value threshold limits and lack of a profit motive.

According to these officials, the statutory dollar-value threshold is very difficult to meet in peer-to-peer cases, since most peer-to-peer infringement is based on the sharing of music, and the major record labels have set \$0.80 as the dollar value of each copy of a song (the officials noted that most successful prosecutions are based on copyright infringement of software applications, because these tend to have a higher dollar value than songs). Proving criminal intent is also often a problem in these cases, since file sharing is a passive act, and in most cases there is no profit motive.

According to Justice officials, federal intellectual property protection efforts do not focus on investigation and prosecution of individual copyright infringers on peer-to-peer networks, but instead they focus on organizations or individuals engaged in massive distribution or reproduction of copyrighted materials. According to these officials, this focus exists because:

- *Federal law enforcement is best suited to focus on large-scale or sophisticated infringers*, including organized groups, large-scale infringers, infringers operating out of numerous jurisdictions and foreign countries, and infringers using sophisticated technology to avoid detection, identification, and apprehension. By and large, individual copyright holders do not have the tools or ability to pursue these types of targets.
- *Copyright holders do not have the legal tools or ability to tackle the organized criminal syndicates and most sophisticated infringers, but they have the tools and ability to target the individual infringer*. While federal law enforcement has the tools, ability, expertise, and will to tackle the most sophisticated infringers, including those operating overseas who are part of a large syndicate and those using sophisticated technology to avoid detection, individual copyright holders have the tools to pursue individual infringers. Congress has provided for civil enforcement actions. Individual copyright holders, mostly through industry associations, have been very active in their pursuit of individual infringers using peer-to-peer applications.
- *Focusing law enforcement and industry on their respective strengths results in maximum impact*. By using both the criminal and civil tools given to law enforcement and industry by Congress, Justice can achieve a more significant impact.
- *Technological limitations pose a challenge*. Given the technology involved, it is challenging to gather the necessary evidence for a successful criminal prosecution of individuals using peer-to-peer applications. For example, it may be possible to prove that someone is offering copyrighted material for download through a peer-to-peer application; but, according to law enforcement officials, it is usually difficult or impossible to determine the number of times files were downloaded.
- *Burden of proof in criminal prosecutions is more onerous*. The criminal statute at issue requires proof of a willful intent and requires that each element of the offense be proven beyond a reasonable doubt. The willful intent is a higher burden than is found in most criminal statutes. By

contrast, the intent element and overall burden of proof is significantly less onerous in civil enforcement.

- *Statutory thresholds favor a federal criminal enforcement focus on the more significant targets.* The thresholds require a retail value of \$2,500 or more for the goods pirated by the infringer. With a valuation of \$0.80 per song that is traded on a peer-to-peer application, federal criminal law enforcement could not be used to target individuals downloading fewer than 3,100 music files, for example. The technological limitations mentioned earlier, combined with the heightened burden of proof, make it challenging to show criminal violations for each of the more than 3,100 downloads.
- *The need for efficient use of resources suggests a focus on large-scale sophisticated targets.* The need for law enforcement to use resources efficiently suggests that federal law enforcement should focus their efforts in a way that yields the greatest impact. For many of the reasons detailed above, federal law enforcement has determined that they can make the biggest impact by focusing on the larger-scale, more sophisticated targets.

According to Justice officials, the recently created Intellectual Property Task Force—headed by the Deputy Chief of Staff and Counselor to the Attorney General, and comprised of several of the highest-ranking department employees who have a variety of subject matter expertise—is charged with examining all aspects of how Justice handles intellectual property issues and with developing recommendations for legislative changes and future activities. One of the issues to be addressed by the task force is the most appropriate use of department resources to ensure that the department has the most effective enforcement strategy.

Federal law enforcement officials did not identify any specific legislative barriers to investigation and prosecution of illegal file sharing on peer-to-peer networks. According to Justice officials, the department's Intellectual Property Task Force will also recommend legislative changes, assuming there is a need for such changes.

Summary

The college and university officials we interviewed are aware of the use of file-sharing applications on their networks, almost all of them have experienced some problems and increased costs as a result of the use of these applications; therefore, they are taking steps to reduce the use of peer-to-peer file-sharing technology on their networks. All of the officials interviewed indicated that their colleges or universities routinely monitor

their networks; and most of them indicated that the institutions also actively monitor their networks, specifically for the use of peer-to-peer file-sharing applications. When infringing use was discovered, all of the officials stated that enforcement actions were taken against the individuals responsible. These actions included issuing warnings to the users, banning them from the network for a period of time, and shaping the bandwidth available for a group of users.

Federal law enforcement officials have been taking action to investigate and prosecute organizations involved in significant copyright infringement. These groups use a wide range of Internet technologies to illegally distribute copyrighted materials over the Internet. Federal law enforcement officials did not identify any specific legislative barriers to investigation and prosecution of illegal file sharing on peer-to-peer networks. According to Justice officials, the department's recently created Intellectual Property Task force will examine how the department handles intellectual property issues and recommend legislative changes, if needed.

Agency Comments and Our Evaluation

In providing comments on a draft of this report, the Deputy Assistant Attorney General, Criminal Division, Department of Justice, provided additional information on a recent international law enforcement effort against online piracy, coordinated by the department's Computer Crime and Intellectual Property Section and the FBI, and presented a detailed description of the department's policy on investigating and prosecuting intellectual property rights infringers on the Internet and on peer-to-peer networks. The Deputy Assistant Attorney General also noted that the department's recently created Intellectual Property Task Force will examine how the department handles intellectual property issues and recommend legislative changes, if needed. We have incorporated this information into this report.

We also received comments (via e-mail) from the unit chief of the Cyber Crime Center on behalf of DHS. The unit chief provided additional details on the number of investigations conducted by the Cyber Crime Center and clarified the center's approach to investigations of individual copyright infringers. Specifically, the unit chief stated that, while the center targets individual violators who are involved in cyber intellectual property piracy on a profit or commercial basis, it does not pursue investigations of individual peer-to-peer file violators, due to the difficulties in meeting the statutory dollar-value threshold in peer-to-peer infringement cases and the lack of a profit motive. We have incorporated these details into this report.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Chairmen and Ranking Minority Members of other Senate and House committees and subcommittees that have jurisdiction and oversight responsibility for Justice and DHS. We are also sending copies to the Attorney General and to the Secretary of Homeland Security. Copies will be made available to others on request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you have any questions concerning this report, please call me at (202) 512-6240 or Mirko J. Dolak, Assistant Director, at (202) 512-6362. We can also be reached by e-mail at koontzl@gao.gov and dolakm@gao.gov, respectively. Key contributors to this report were Jason B. Bakelar, Barbara S. Collier, Nancy E. Glover, Lori D. Martinez, Morgan F. Walts, and Monica L. Wolford.



Linda D. Koontz
Director, Information Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to describe (1) the views of major universities on the extent of problems experienced with student use of file-sharing software applications, as well as the actions that the universities are taking to deal with them and (2) the actions that federal enforcement agencies have taken to address the issue of copyright infringement on peer-to-peer networks, as well as agency views on any legislative barriers to dealing with these problems.

To describe the views of college and university officials, we conducted structured interviews with a judgmental sample of large colleges and universities. The interview contained 35 questions referring to (1) the extent to which the college or university monitors its network or networks and the impact of the use of file-sharing applications on the network, (2) estimates of the number of students using file-sharing applications and the number of files shared or transferred over the network, (3) the discovery of nodes or mini-Napsters on the network and response of the university to their existence, (4) the discovery of file-sharing applications on the network and response of the university to their use, and (5) the actions taken by the college or university to address copyright infringement and the use of file-sharing applications on its networks.

We pretested the content of the interview with chief information officers (CIO) of four major colleges and universities. During the pretest, we asked the CIOs to judge the following:

- how willing the CIOs would be to participate in the interview, particularly given the sensitive nature of some of the information requested;
- whether the meaning and intent of each question was clear and unambiguous;
- whether the CIOs were likely to know the information asked, and if the questions should be addressed to someone in a different position; and
- whether any of the questions were redundant.

We made changes to the content and format of the final structured interview based on pretest results.

To administer the structured interviews, we selected 45 colleges and universities from the Department of Education Integrated Postsecondary Education Data System. The colleges and universities were judgmentally selected from among large public and private degree-granting colleges and

universities in each of eight geographic regions of the United States that provide Internet access to students in university administered housing.¹ Of the 45 colleges and universities selected and contacted, 13 agreed to participate in the interview. We then analyzed the interview responses. Our analysis provides details on the responses of the 13 college and university officials we interviewed; however, because we did not randomly select interviewees, our results cannot be generalized to all colleges and universities.

To describe federal law enforcement efforts and agency views related to copyright infringement on peer-to-peer networks, we analyzed budget and program documents from the Justice Computer Crime and Intellectual Property Section; the Federal Bureau of Investigation (FBI) Cyber Division; and the U.S. Immigration and Customs Enforcement's Cyber Crimes Center, under the Department of Homeland Security. We also reviewed agency documents related to the efforts of other organizations that support the investigation and prosecution of copyright infringement, including the Department of State's International Law Enforcement Academies; the Department of Commerce's International Trade Administration; and the Intellectual Property Rights Coordination Center and the National Intellectual Property Law Enforcement Coordination Council.

We performed our work between May 2003 and April 2004 in Washington, D.C. Our work was conducted in accordance with generally accepted government auditing standards.

¹The universities that were involved in pretesting the interview questions were not included in the interviews.

Appendix II: Description of File Sharing and Peer-to-Peer Networks

Peer-to-peer file-sharing programs represent a major change in the way Internet users find and exchange information. Under the traditional Internet client/server model, the access to information and services is accomplished by the interaction between users (clients) and servers—usually Web sites or portals. A client is defined as a requester of services, and a server is defined as the provider of services. Unlike the client/server model, the peer-to-peer model enables consenting users—or peers—to directly interact and share information with each other’s computer without the intervention of a server. A common characteristic of peer-to-peer programs is that they build virtual networks with their own mechanisms for routing message traffic.¹

The ability of peer-to-peer networks to provide services and connect users directly has resulted in a large number² of powerful applications being built around this model.³ Among the uses of peer-to-peer technology are the following:

- *File sharing*, which includes applications such as Napster and KaZaA, along with commercial applications such as NextPage.⁴ File-sharing applications work by making selected files on a user’s computer available for download by anyone else using similar software.
- *Instant messaging*, which includes applications that enable online users to communicate immediately through text messages. Commercial vendors include America Online, Microsoft, and Jabber.
- *Distributed computing*, which includes applications that use the idle processing power of many computers. The University of California–

¹Matei Ripenau, Ian Foster, and Adriana Iamnitchi, “Mapping the Gnutella Network: Properties of Large Scale Peer-to-Peer Systems and Implication for System Design,” *IEEE Internet Computing*, vol. 6, no. 1 (January–February 2002). (<http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf>)

²Zeropaid.com, a file-sharing portal, lists 88 different peer-to-peer file-sharing programs available for download. (<http://www.zeropaid.com/php/filessharing.php>)

³Geoffrey Fox and Shrideep Pallickara, “Peer-to-Peer Interactions in Web Brokering Systems,” *Ubiquity*, vol. 3, no. 15 (May 28–June 3, 2002) (published by Association of Computer Machinery). (http://www.acm.org/ubiquity/views/g_fox_2.html)

⁴NextPage provides information-intensive corporations with customized peer-to-peer file-sharing networks. It enables users to manage, access, and exchange content across distributed servers on intranets and via the Internet.

Berkeley's SETI@home project uses the idle time on volunteers' computers to analyze radio signal data.

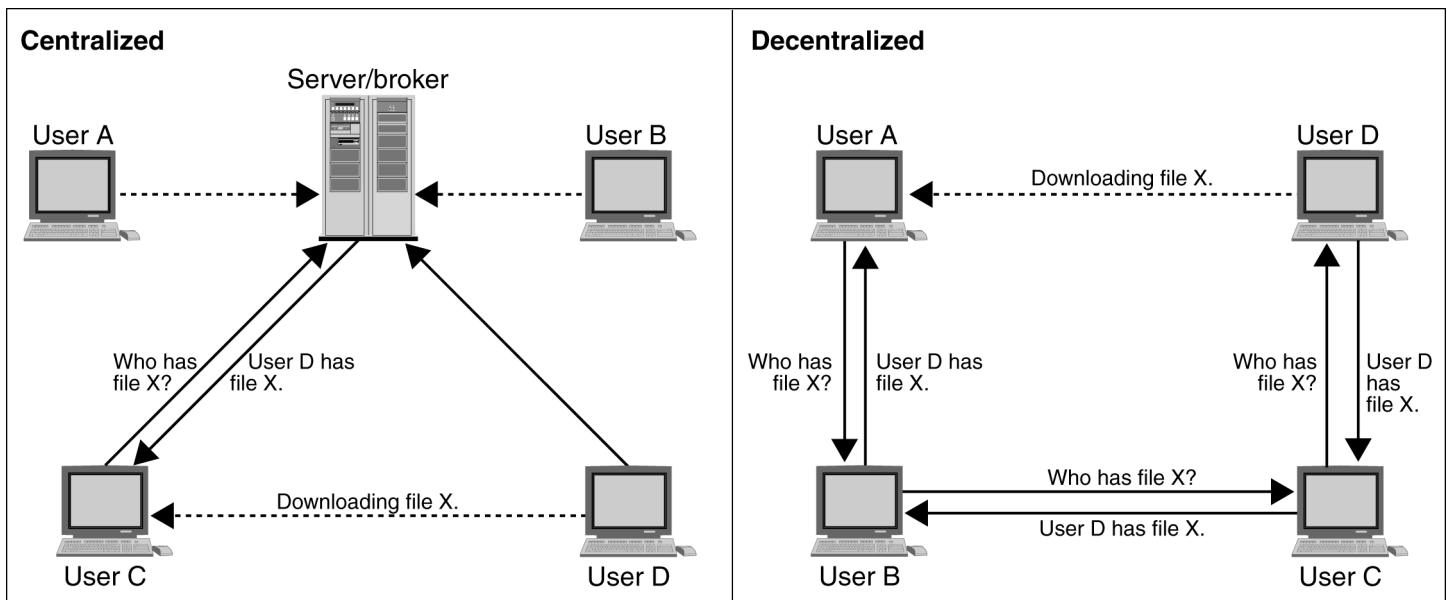
- *Collaboration applications*, which enable teams in different geographic areas to work together and increase productivity. For example, the Groove application can access data on traditional corporate networks and on nontraditional devices such as personal digital assistants and handheld devices.

As shown in figure 7,⁵ there are two main models of peer-to-peer networks: (1) the centralized model, based on a central server, or broker, that directs traffic between individual registered users and (2) the decentralized model, based on the Gnutella⁶ network, in which individuals find and interact directly with each other.

⁵Illustration adapted by Lt. Col. Mark Bontrager from original by Bob Knighten, "Peer-to-Peer Computing," briefing to Peer-to-Peer Working Groups (August 24, 2000), in Mark D. Bontrager, *Peering into the Future: Peer-to-Peer Technology as a Model for Distributed Joint Battlespace Intelligence Dissemination and Operational Tasking*, Thesis, School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, Alabama (June 2001).

⁶According to LimeWire LLC, the developer of a popular file-sharing program, Gnutella was originally designed by Nullsoft, a subsidiary of America Online. The development of the Gnutella protocol was halted by America Online management shortly after the protocol was made available to the public. Using downloads, programmers reverse-engineered the software and created their own Gnutella software packages. (<http://www.limewire.com/index.jsp/p2p>)

Figure 7: Peer-to-Peer Models



Source: Mark Bontrger, Bob Knighten.

Note: Adapted from Mark Bontrager's adaptation of original by Bob Knighten.

As figure 7 shows, the centralized model relies on a central server/broker to maintain directories of shared files stored on the respective computers of the registered users of the peer-to-peer network. When user C submits a request for a file, the server/broker creates a list of files matching the search request by checking the request with its database of files belonging to registered users currently connected to the network. The broker then displays that list to user C, who can then select the desired file from the list and open a direct link with user D's computer, which currently has the file. The download of the actual file takes place directly from user D to user C.

The broker model was used by Napster, the original peer-to-peer network; it facilitated mass sharing of copyrighted material by combining the file names held by thousands of users into a searchable directory that enabled users to connect with each other and download MP3 encoded music files.

The broker model made Napster vulnerable to legal challenges⁷ and eventually led to its demise in September 2002.

Although Napster was litigated out of existence and its users fragmented among many alternative peer-to-peer services, most current-generation peer-to-peer networks are not dependent on the server/broker that was the central feature of the Napster services, so, according to Gartner,⁸ these networks are less vulnerable to litigation from copyright owners.

In the decentralized model, no brokers keep track of users and their files. To share files using the decentralized model, user A starts with a networked computer equipped with a Gnutella file-sharing program, such as KaZaA or BearShare. User A connects to user B, user B to user C, user C to user D, and so on. Once user A's computer has announced that it is "alive" to the various members of the peer network, it can search the contents of the shared directories of the peer network members. The search request is sent to all members of the network, starting with user B, who will each, in turn, send the request to the computers to which they are connected, and so on. If one of the computers in the peer network (for example, user D) has a file that matches the request, it transmits the file information (name, size, type, etc.) back through all the computers in the pathway toward user A, where a list of files matching the search request appears on user A's computer through the file-sharing program. User A will then be able to open a connection with user D and download the file directly from user D's computer.⁹

One of the key features of Napster and the current generation of decentralized peer-to-peer technologies is their use of a virtual name space. A virtual name space dynamically associates user-created names with the Internet address of whatever Internet-connected computer users happen to be using when they log on.¹⁰ The virtual name space facilitates point-to-point interaction between individuals, because it removes the need for users and their computers to know the addresses and locations of

⁷*A&M Records v. Napster*, 114 F.Supp.2d 896 (N.D. Cal. 2000).

⁸Lydia Leong, "RIAA vs. Verizon, Implications for ISPs," Gartner (Oct. 24, 2002).

⁹LimeWire, *Modern Peer-to-Peer File sharing over the Internet*.
(<http://www.limewire.com/index.jsp/p2p>)

¹⁰S. Hayward and R. Batchelder, "Peer-to-Peer: Something Old, Something New," Gartner (Apr. 10, 2001).

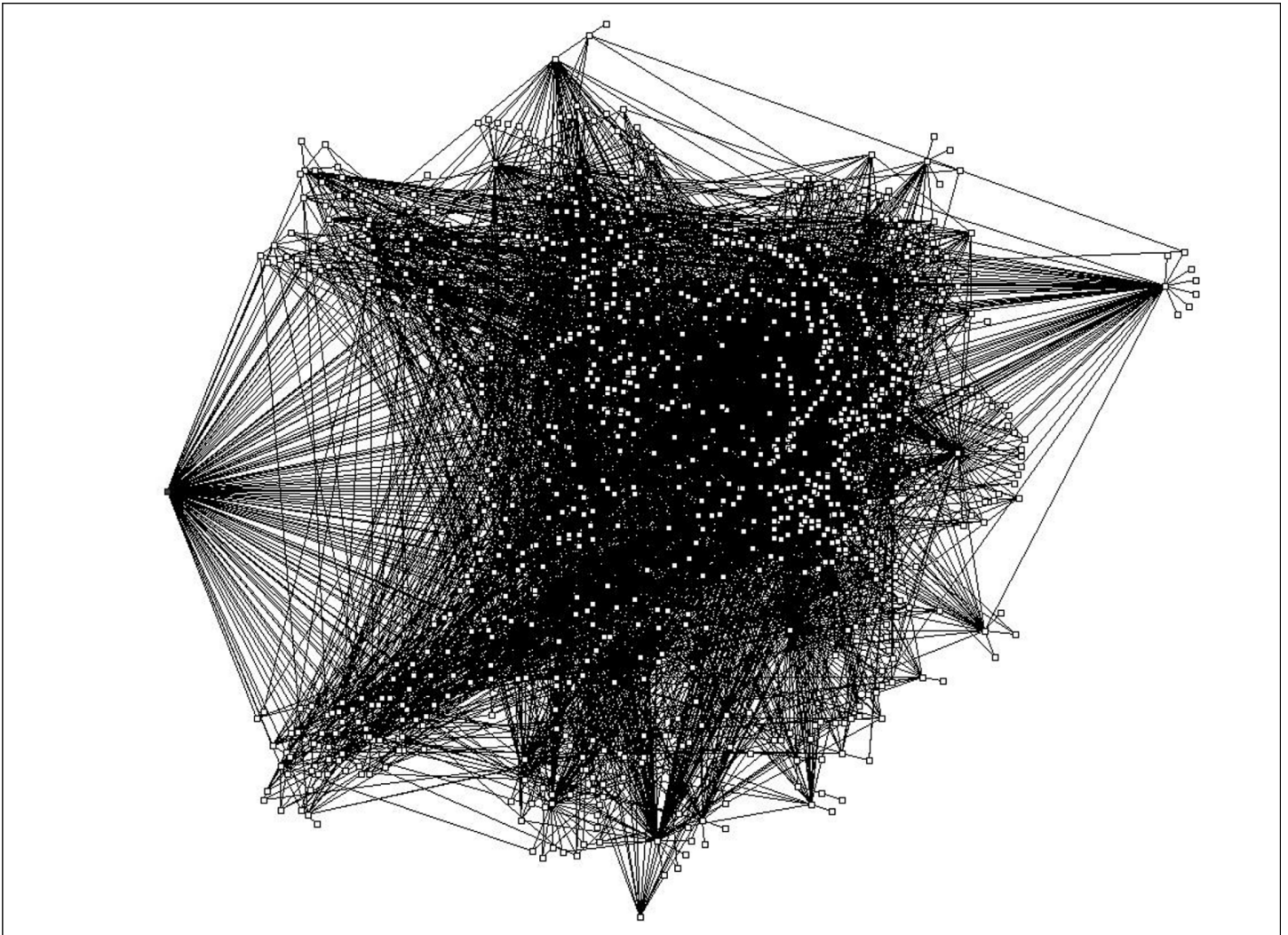
other users; the virtual name space can, to a certain extent, preserve users' anonymity and provide information on whether a user is or is not connected to the Internet at a given moment.¹¹

The file-sharing networks that result from the use of peer-to-peer technology are both extensive and complex. Figure 8 shows a map, or topology, of a Gnutella network whose connections were mapped by a network visualization tool.¹² The map, created in December 2000, shows 1,026 nodes (computers connected to more than one computer) and 3,752 edges (computers on the edge of the network connected to a single computer). This map is a snapshot showing a network in existence at a given moment; these networks change constantly as users join and depart them.

¹¹Peer-to-peer users may appear to be, but are not, anonymous. Law enforcement agents may identify users' Internet addresses during the file-sharing process and obtain, under a court order, their identities from their Internet service providers.

¹²Mihajlo A. Jovanovic, Fred S. Annexstein, and Kenneth A. Berman, *Scalability Issues in Large Peer-to-Peer Networks: A Case Study of Gnutella*, University of Cincinnati Technical Report (2001). (<http://www.ececs.uc.edu/~mjovanov/Research/paper.html>)

Figure 8: Topology of a Gnutella Network



Source: Mihajlo A. Jovanovic, Fred S. Annexstein, and Kenneth A. Berman, Laboratory of Networks and Applied Graph Theory, University of Cincinnati.

Appendix III: Key and Supporting Federal Agencies Involved in the Investigation and Prosecution of Copyright Infringement

The emergence of the Internet as a principal medium for copyright infringement and other crimes has led to the development of new divisions within the federal government that are specifically trained to deal with cybercrime issues. These divisions, as well as other entities that are involved in combating copyright infringement, fulfill three main roles: investigation, prosecution, and support. The investigation role includes activities related to gathering and analyzing evidence related to suspected copyright infringement, while the prosecution role includes activities related to the institution and continuance of a criminal suit against an offender. The support role includes activities that are not directly involved in either investigation or prosecution, but which assist other organizations in these activities. Support activities include providing specialized training, producing reports specifically pertaining to intellectual property rights and copyright infringement, observing international trade agreements, and providing investigation leads and supporting evidence.

Investigating Agencies

Federal agencies involved in the investigation process of copyright infringement include the following:

Department of Homeland Security

U.S. Immigration and Customs Enforcement, Cyber Crimes Center. The Cyber Crimes Center, independently or in conjunction with Immigration and Customs Enforcement field offices, investigates domestic and international criminal activities conducted on or facilitated by the Internet. The organization's responsibilities include investigating money laundering, drug trafficking, intellectual property rights violations, arms trafficking, and child pornography cases, and they provide computer forensics support to other agencies. For fiscal year 2002, the U.S. Customs Service¹ referred 57 investigative matters related to intellectual property rights cases to the U.S. Attorneys Offices. Of these cases, 37 involving 54 defendants were resolved or terminated.

Department of Justice

FBI Cyber Division. The Cyber Division coordinates, supervises, and facilitates the FBI's investigation of federal violations in which the Internet, computer systems, and networks are exploited as the principal

¹On March 1, 2003 the U.S. Customs Service was reconfigured into two agencies within DHS, at which time the Office of Investigations and the Cyber Crimes Center became part of U.S. Immigration and Customs Enforcement.

instruments or targets of criminal, foreign intelligence, or terrorism activity and for which the use of such systems is essential to that activity. For fiscal year 2003, the Cyber Division investigated 596 cases involving intellectual property rights. Of these cases, 160 were related specifically to software copyright infringement and 111 were related to other types of copyright infringement. The results of these investigations include 92 indictments and 95 convictions/pretrial diversions.

Prosecuting Agencies

Federal agencies involved in the prosecution process of copyright infringement include the following:

Department of Justice

Computer Crime and Intellectual Property Section. The Computer Crime and Intellectual Property Section consists of 38 attorneys who focus exclusively on computer and intellectual property crime, including (1) prosecuting cybercrime and intellectual property cases; (2) advising and training local, state, and federal prosecutors and investigators in network attacks, computer search and seizure, and intellectual property law; and (3) coordinating international enforcement and outreach efforts to combat intellectual property and computer crime worldwide.

Computer Hacking and Intellectual Property Units. Computer Hacking and Intellectual Property units are comprised of highly trained prosecutors and staff who are dedicated primarily to prosecuting high-tech crimes, including intellectual property offenses. There are 13 Computer Hacking and Intellectual Property units located in U.S. Attorneys Offices across the nation. Each unit is comprised of between four and six prosecutors and dedicated support staff.

Computer and Telecommunication Coordinator Network. The Computer and Telecommunication Coordinator program consists of prosecutors specifically trained to address the range of novel and complex legal issues related to high tech and intellectual property crime, with general responsibility for prosecuting computer crime, acting as a technical advisor and liaison, and providing training and outreach. The Computer and Telecommunication Coordinator program is made up of more than 200 Assistant U.S. Attorneys, with at least one prosecutor who is part of the program in each of the 94 U.S. Attorneys Offices.

U.S. Attorneys Offices. The U.S. Attorneys serve as the nation's principal federal litigators under the direction of the U.S. Attorney General. U.S. Attorneys conduct most of the trial work in which the United States is a

party and have responsibility for the prosecution of criminal cases brought by the federal government, the prosecution and defense of civil cases in which the United States is a party, and the collection of debts owed the federal government which are administratively uncollectible. There are 94 U.S. Attorneys stationed throughout the United States, Puerto Rico, the Virgin Islands, Guam, and the Northern Mariana Islands. For fiscal year 2002, the U.S. Attorneys Offices received 75 referrals involving investigative matters for Title 18, U.S.C., Section 2319—Criminal Infringement of a Copyright—and 28 cases involving 56 defendants were resolved or terminated.

Supporting Agencies

Department of Homeland Security

U.S. Immigration and Customs Enforcement, Intellectual Property Rights Coordination Center. The Center is a multiagency organization that serves as a clearinghouse for information and investigative leads provided by the general public and industry, as well as being a channel for law enforcement to obtain cooperation from industry.

Department of Justice

The Criminal Division, through its Overseas Prosecutorial Development, Assistance and Training Office and its International Criminal Investigation Training Assistance Programs, provides training and assistance to foreign law enforcement and foreign governments to foster the robust protection of intellectual property rights in foreign countries.

Federal Bureau of Investigation

Through its legal attaches located in foreign countries, the FBI fosters the protection of intellectual property rights in foreign countries and assists U.S. prosecutions of intellectual property violations that have foreign roots.

Department of State

International Law Enforcement Academies. The academies foster a cooperative law enforcement partnership and involvement between the U.S. and participating nations to counter the threat of international crime within a specific region. The academies develop foreign police managers' abilities to handle a broad spectrum of contemporary law enforcement issues, including specialized training courses in fighting intellectual property rights crime, and increases their capacity to investigate crime and criminal organizations. As of 2003, academies were operating in Roswell,

Appendix III: Key and Supporting Federal Agencies Involved in the Investigation and Prosecution of Copyright Infringement

New Mexico; Budapest, Hungary; Bangkok, Thailand; and Gaborone, Botswana.

U.S. Department of Commerce

International Trade Administration. The administration monitors foreign governments' compliance and implementation with international trade agreements, especially those pertaining to intellectual property rights enforcement.

Others

National Intellectual Property Law Enforcement Coordination Council. The Council's mission is to coordinate domestic and international intellectual property law enforcement among federal and foreign entities, including law enforcement liaison, training coordination, industry and other outreach, and to increase public awareness. The Council consists of members from several agencies, including the Director of the U.S. Patent and Trademark Office (co-chair); the Assistant Attorney General of the Department of Justice's Criminal Division (co-chair); the Undersecretary of State for Economics, Business, and Agricultural Affairs; the Deputy U.S. Trade Representative; the Commissioner of Customs; and the Undersecretary of Commerce for International Trade. The council is required to report annually on its coordination activities to the President and to the Appropriations and Judiciary Committees of the House and Senate.

Appendix IV: Comments from the Department of Justice



U.S. Department of Justice

Criminal Division

Deputy Assistant Attorney General

Washington, D.C. 20530

April 30, 2004

Ms. Linda D. Koontz
Director, Information Management Issues
US General Accounting Office
441 G Street N.W.
Washington, DC 20548

Dear Ms. Koontz:

Thank you for providing the Criminal Division with the opportunity to present the Department of Justice's enforcement efforts in the area of intellectual property crime, particularly related to copyright infringement using Internet technologies such as peer-to-peer applications.

On April 21, 2004, the Department led the single largest international enforcement effort ever undertaken against online piracy - Operation Fastlink. Operation Fastlink involved the simultaneous execution of searches in the United States and ten foreign countries. As a result of the coordination by the Department's Computer Crime and Intellectual Property Section and the FBI, in one 24 hour period over 120 searches were executed across multiple time zones. In addition to the United States, searches were executed in Belgium, Denmark, France, Germany, Hungary, Israel, the Netherlands, Singapore, Sweden, Great Britain, and Northern Ireland. As a result, over 100 individuals believed to be engaged in online piracy have been identified, many of them high-level members or leaders of online piracy release groups that specialize in distributing high-quality pirated movies, music, games, and software over the Internet. More than 200 computers were seized worldwide, including over 30 computer servers which function as storage and distribution hubs for many of the online piracy groups targeted by this Operation. As noted, this is the single largest law enforcement effort ever undertaken against online piracy, and it is the most recent, and best, example of the approach law enforcement is taking toward online piracy.¹

¹The Recording Industry Association of America issued a press release regarding Operation Fastlink, praising the effectiveness and commitment of the Department's enforcement effort:

We appreciate and applaud the work of the U.S. Justice Department, Attorney General Ashcroft and the entire

The Department's intellectual property criminal enforcement efforts focus on large-scale and sophisticated infringers – for example, organizations or individuals engaged in massive distribution or reproduction of copyrighted materials. This focus exists because (1) federal law enforcement is best-suited to the identification, targeting, and dismantling of significant or sophisticated criminal organizations; (2) copyright holders typically do not have the ability or the tools to focus on the significant and sophisticated organized targets whose activities and members span the globe – by contrast, they typically do have the legal tools, ability, and will to pursue the individual copyright infringers; (3) focusing law enforcement and industry efforts on their respective areas of strength results in a more significant overall impact; (4) technological limitations make it challenging to pursue individual infringers using peer-to-peer applications; (5) the burden of proof in criminal enforcement is significantly more difficult to meet than the burden of proof in civil enforcement; (6) statutory thresholds, involving the value of pirated goods, tend to favor federal enforcement directed at large-scale or sophisticated infringement activity rather than individual infringers; and finally (7) the need for efficient use of resources suggests that federal resources should be used to pursue that criminal conduct which has the most adverse impact on copyright holders.

(1) federal law enforcement is best-suited to focus on large-scale or sophisticated infringers: federal law enforcement is best-suited to focus on sophisticated infringers, including organized groups, large-scale infringers, infringers operating out of numerous jurisdictions and foreign countries, and infringers using sophisticated technology to avoid detection, identification, and apprehension. By and large, individual copyright holders do not have the tools or ability to pursue these types of perpetrators.

(2) copyright holders do not have the legal tools or ability to tackle the organized criminal syndicates and most sophisticated infringers, but they do have the tools and ability to target the individual infringers: Federal law enforcement has the tools, ability, expertise, and will to tackle the most sophisticated infringers, including those operating overseas who are part of large syndicates and those using sophisticated technology to avoid detection; whereas individual copyright holders have the tools to pursue individual infringers. Congress has provided for civil copyright enforcement actions, and individual copyright holders, mostly through industry associations, have been very active in their pursuit of individual infringers using peer-to-peer applications. Recent media reports suggest those civil enforcement actions have had a significant impact on reducing illegal peer-to-peer file sharing of copyrighted works.

Administration. They have undertaken and spearheaded an unprecedented, international initiative that strikes a forceful blow at global piracy operations that have been wreaking enormous damage on creative communities around the world. This is a sizeable achievement and creators all over the world owe a debt of gratitude.

See <http://www.pcworld.com/news/article/0,aid,114086,00.asp> and <http://www.cnn.com/2004/TECH/internet/04/26/downloading.music.ap/index.html>.

(3) focusing law enforcement and industry on their respective strengths results in maximum impact: by using both the criminal and civil tools given by Congress to law enforcement and industry, respectively, we can achieve a more significant impact.

(4) technological limitations pose a challenge: given the technology involved in peer-to-peer applications, it is challenging to gather the necessary evidence for a successful criminal prosecution of individuals using peer-to-peer applications. For example, it may be possible to prove that someone is offering copyrighted material for download through a peer-to-peer application, but it is usually difficult and sometimes impossible to determine the number of times files were downloaded.

(5) burden of proof in criminal prosecutions is more onerous: the criminal infringement statute requires proof of a willful intent, and each element of the offense must be proven beyond a reasonable doubt. Willful intent is a higher burden than is found in most criminal statutes. By contrast, the intent element and overall burden of proof is significantly less onerous in civil enforcement.

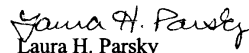
(6) statutory thresholds favor a federal criminal enforcement focus on the more sophisticated targets: the statutory thresholds require a retail value of \$2,500 or more of the goods pirated by the infringer. Consequently, if each song that is traded on a peer-to-peer application is valued at \$0.80, federal criminal law enforcement cannot be used to target individuals downloading fewer than 3,100 music files.

(7) the need for efficient use of resources suggests a focus on large-scale, sophisticated targets: the resource limitations faced by law enforcement generally suggest that federal law enforcement should focus its efforts in a way that yields the greatest impact. For many of the reasons detailed above, federal law enforcement has determined that it can make the biggest impact by focusing on the larger-scale, more sophisticated targets.

The Department of Justice very recently created an Intellectual Property Task Force, headed by the Deputy Chief of Staff and Counselor to the Attorney General. The Task Force, comprised of several of the highest ranking Department executives with varied subject matter expertise, is charged with examining all aspects of how the Department of Justice handles intellectual property issues and with developing recommendations for future activity. One of the issues to be addressed by the Task Force is the most appropriate use of Departmental resources to ensure the Department has in place the most effective enforcement strategy. The Task Force will also recommend legislative changes, assuming current practice identifies the need for such changes.

Thank you again for the opportunity to share with the General Accounting Office our criminal enforcement efforts to address the growing problem of online piracy. The Department fully recognizes the deleterious effect of this piracy on the economic health of our most innovative companies, our talented inventors and entrepreneurs, and all those Americans employed by affected industries. We are strongly committed to using criminal enforcement tools -- appropriately and in the most effective manner -- to send the clear message that the theft of intellectual property will not be tolerated.

Sincerely,


Laura H. Parsky
Deputy Assistant Attorney General

Glossary

BearShare	A file-sharing program for Gnutella networks. BearShare supports the trading of text, images, audio, video, and software files with any other user of the network.
broker	In the peer-to-peer environment, an intermediary computer that coordinates and manages requests between client computers.
client-server	A networking model in which a collection of nodes (client computers) request and obtain services from a server node (server computer).
Gnutella	A file-sharing program based on the Gnutella protocol. Gnutella enables users to directly share files with one another. Unlike Napster, Gnutella-based programs do not rely on a central server to find files.
Gnutella protocol	Decentralized group membership and search protocol, typically used for file sharing. Gnutella file-sharing programs build a virtual network of participating users.
Instant messaging (IM)	A popular method of Internet communication that allows for an instantaneous transmission of messages to other users who are logged into the same IM service. America Online's Instant Messenger and the Microsoft Network Messenger are among the most popular instant messaging programs.
Internet Protocol (IP) address	IP address. A number that uniquely identifies a computer connected to the Internet to other computers.
KaZaA	A file-sharing program using a proprietary peer-to-peer protocol to share files among users on the network. Through a distributed self-organizing network, KaZaA requires no broker or central server like Napster.
LimeWire	A file-sharing program running on Gnutella networks. It is open standard software running on an open protocol and is free for public use.
MP3	Moving Pictures Experts Group (MPEG) MPEG-1 Audio Layer-3. A widely used standard for compressing and transmitting music in digital format across Internet. MP3 can compress file sizes at a ratio of about 10:1 while preserving sound quality.
node	A computer or a device that is connected to a network. Every node has a unique network address.

peer	A network node that may function as a client or as a server. In the peer-to-peer environment, peer computers are also called servents, since they perform tasks associated with both servers and clients.
server	A computer that interconnects client computers, providing them with services and information; a component of the client-server model. A Web server is one type of server.
SETI@home	Search for extraterrestrial intelligence at home. A distributed computing project, SETI@home uses data collected by the Arecibo Telescope in Puerto Rico. The project takes advantage of the unused computing capacity of personal computers. As of February 2000, the project encompassed 1.6 million participants in 224 countries.
topology	The general structure—or map—of a network. It shows the computers and the links between them.
virtual	Having the properties of x while not being x. For example, “virtual reality” is an artificial or simulated environment that appears to be real to the casual observer.
virtual name space (VNS)	Internet addressing and naming system. In the peer-to-peer environment, VNS dynamically associates names created by users with the IP addresses assigned by their Internet services providers to their computers.
World Wide Web	A worldwide client-server system for searching and retrieving information across the Internet. Also known as WWW or the Web.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
 TDD: (202) 512-2537
 Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548