

**Public Workshop: Peer-to-Peer File-Sharing Technology: Consumer
Protection and Competition Issues**

P2P File-Sharing Workshop – Comment, P034517

Exhibits of
The Recording Industry Association of America (RIAA)
November 15, 2004

P2P File-Sharing Workshop – Comment, P034517

Attachments for Comments of
The Recording Industry Association of America (RIAA)
November 15, 2004

Articles

“Justice Department Announces International Internet Piracy Sweep,” Department of Justice press release, 4/22/04	1
“New TruSecure Research Offers Corporations Insight into Potential Threats and Their Impact in 2004,” TruSecure Press Release, 12/29/03	2
“What’s in Your Shared Folder?” Slyck, 7/30/04	3

Governmental Notices and Orders

P2P On Government Computers – Orders and Concerns	4
“Commerce IT Security Policy on Peer-to-Peer File Sharing,” U.S. Department of Commerce, 5/21/04	5
“FY 2004 Reporting Instructions for the Federal Information Security Management Act,” Office of Management and Budget, 8/23/04	6
“Interim Guidance on Peer-to-Peer Software and Copyright,” U.S. Department of Agriculture	7
“Personal Use Policies and ‘File Sharing’ Technology,” Office of Management and Budget, 9/8/04	8
“Use of Peer-to-Peer File Sharing Technology,” U.S. Department of Justice, 9/17/04	9
U.S. Army, Army News Service, <i>Downloading shared files threatens security</i> (4/22/04)	10
Executive Order S-16-04, State of California, Executive Department, 9/16/04	11
“Governor pushed for file sharing warning,” The Diamondback, 1/30/04	12
“Traffic to block outbound to the Internet,” State of Michigan	13

Letters

Letter to FTC from Senators Leahy, Hatch, Boxer, Stevens, and Smith, 5/4/04	14
Letter to P2P Executives from Senators Graham, Feinstein, Durbin, Smith, Cornyn, and Boxer, 11/12/03	15
Letter to P2P United from 47 U.S. Attorneys General, 8/5/04	16

Notices

FBI Cyber Education Letter (http://www.fbi.gov/cyberinvest/cyberedletter.htm)	17
“File-sharing: A Fair Share? Maybe Not,” FTC Consumer Alert, July 2003	18

Reports

“File-Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography,” GAO Report to the Chairman and Ranking Minority Member, Committee on Government Reform, House of Representatives, February 2003	19
“File-Sharing: Selected Universities Report Taking Action to Reduce Copyright Infringement,” GAO Report to Congressional Requesters, May 2004	20
“Peer-to-Peer (P2P) Piracy on University Campuses: An Update,” Joint Committee of the Higher Education and Entertainment Communities report to the Subcommittee on Courts, the Internet, and Intellectual Property, House Judiciary Committee, October 2004	21
“Peer-to-Peer Software Providers’ Liability under Section 5 of the FTC Act” (4/27/04).....	22
“Progress during the Past Academic Year Addressing Illegal File Sharing on College Campuses,” Joint Committee of the Higher Education and Entertainment Communities report to the Subcommittee on Courts, the Internet, and Intellectual Property, House Judiciary Committee, August, 2004.....	23

Studies

“Digital Music: ‘Fear-to-Peer’ Tactics Pave Way for Download Revenue,” eMarketer Spotlight Report, January 2004	24
“From Discs to Downloads,” Forrester Research report, August 2003	25
Palisade Systems study, 3/20/03	26
“P2P Fear and Loathing: Operational Hazards of File Trading Networks,” John Hale, Nicholas Davies, James Arrowood and Gavin Manes, September 2002	27
“Usability and privacy: a study of Kazaa P2P file-sharing,” Nathaniel Good and Aaron Krekelberg, 6/5/04.....	28



Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, APRIL 22, 2004
WWW.USDOJ.GOV

CRM
(202) 514-2008
TDD (202) 514-1888

JUSTICE DEPARTMENT ANNOUNCES INTERNATIONAL INTERNET PIRACY SWEEP

'Operation Fastlink' Is The Largest Global Enforcement Action Ever Undertaken Against Online Piracy

WASHINGTON, D.C. - Attorney General John Ashcroft announced today the most far-reaching and aggressive enforcement action ever undertaken against organizations involved in illegal intellectual property piracy over the Internet. Beginning yesterday morning, law enforcement from 10 countries and the United States conducted over 120 searches worldwide to dismantle some of the most well-known and prolific online piracy organizations.

"Intellectual property theft is a global problem that hurts economies around the world. To be effective, we must respond globally," Attorney General Ashcroft said. "In the past 24 hours, working closely with our foreign law enforcement counterparts, we have moved aggressively to strike at the very core of the international online piracy world."

Operation Fastlink is the culmination of four separate undercover investigations simultaneously being conducted by the FBI, coordinated by the FBI Cyber Division, and the U.S. Department of Justice, coordinated by the Computer Crimes and Intellectual Property Section (CCIPS) of the Criminal Division. As a result of Fastlink, over 120 total searches have been executed in the past 24 hours in 27 states and in 10 foreign countries. Foreign searches were conducted in Belgium, Denmark, France, Germany, Hungary, Israel, the Netherlands, Singapore, Sweden as well as Great Britain and Northern Ireland. Operation Fastlink is the largest multi-national law enforcement effort ever directed at online piracy. Nearly 100 individuals worldwide have been identified by the investigation to date, many of whom are the leaders or high-level members of various international piracy organizations. As the investigations continue, additional targets will be identified and pursued.

"The amount of international coordination and cooperation in this effort is unprecedented and will send a clear and unmistakable message to those individuals and organizations dedicated to piracy that they will no longer be protected by geographic boundaries," Attorney General Ashcroft said. "We are committed to combating this theft and will pursue these thieves regardless of their location."

In addition to attacking piracy globally, Operation Fastlink struck at all facets of the illegal software, game, movie, and music trade online, which is commonly referred to as the "warez scene." The investigations focused on individuals and organizations, known as "warez" release groups, that

specialize in the Internet distribution of pirated materials. Release groups are the first-providers - the original source for most of the pirated works traded or distributed online. Once a release group prepares a stolen work for distribution, the material is distributed in minutes to secure, top-level warez servers and made available to a select clientele. From there, within a matter of hours, the pirated works are further distributed throughout the world, ending up on public channels on IRC and peer-to-peer file sharing networks accessible to anyone with Internet access.

The top release groups are hierarchical, highly structured organizations with leadership positions that control day-to-day operations, recruit new members and manage the group's various computer archive sites. These groups exist solely to engage in piracy and compete with each other to be the first to place a newly pirated work onto the Internet - often before the work is legitimately available to the public. Highly sophisticated technological measures are employed by the groups to shield their illegal activity from victims and law enforcement.

The release groups targeted by Fastlink specialize in the distribution of all types of pirated works including utility and application software, movies, music and games. Among the groups targeted by Fastlink are well-known organizations such as Fairlight, Kalisto, Echelon, Class and Project X, all of which specialized in pirating computer games, and music release groups such as APC. The enforcement action announced today is expected to dismantle many of these international warez syndicates and significantly impact the illicit operations of others.

Operation Fastlink also resulted in the seizure of more than 200 computers, including 30 computer servers that functioned as storage and distribution hubs. These servers collectively contain hundreds of thousands of copies of pirated works. One of the storage and distribution servers seized in the United States reportedly contained 65,000 separate pirated titles. Other servers seized, so-called "elite" sites, contain the most highly coveted and valuable "new releases," many of which were distributed to the warez scene before they are commercially available to the general public. Although access to these elite servers is limited, authorized users frequently provide the first copies of new releases that are traded and distributed online throughout the world within hours of their initial illegal release. Conservative estimates of the value of the pirated works seized easily exceed \$50 million. Conservative projections of the losses to industry attributable to these distribution hubs are in the hundreds of millions of dollars.

Operation Fastlink has been conducted under the direction of the Federal Bureau of Investigation, and agents from 30 separate field offices across the nation were involved in the enforcement action. The investigation has been coordinated with the Justice Department's CCIPS Section and federal prosecutors from 42 separate United States Attorneys' Offices nationwide.

The ongoing investigations were assisted by various intellectual property trade associations, including the Business Software Alliance, the Entertainment Software Association, the Motion Picture Association of America and the Recording Industry Association of America.

###

04-263


[Web view](#)
[Management](#)
[Calendar of Events](#)
[Press Center](#)
[Press Releases](#)
[News Clips](#)
[Press Kit](#)
[Partners](#)
[Investors](#)
[Milestones](#)
[Awards](#)
[International](#)

New TruSecure Research Offers Corporations Insight into Potential Threats and Their Impact in 2004

Peer-to-Peer Applications, Spyware and Trojans Now Pose Larger Threat to Security Administrators and Corporate Networks According to Threat Analysis

Herndon, VA - December 29, 2003 - TruSecure® Corporation, the leading provider of intelligent risk management products and services, today unveiled new research giving security administrators and corporations insight into emerging threats and expected impact in 2004. The research is based on months of malicious code data from the Wild List Organization, a division of ICSA Labs®, and other research performed by TruSecure. White papers describing this research are now available for download:

- 2003/2004 Trends and Predictions in Network Security
- WildTrends 2003: A Look at Virus Trends in 2003 and a Few Predictions for 2004

"While it remains true that only a handful of threats over the course of any year combine the ability to exploit vulnerabilities with a costly payload, we are seeing new and more dangerous threats emerge," said Bruce Hughes, director of malicious code research at TruSecure's ICSA Labs. "Boot sector and macro viruses continue to rapidly decline in their prevalence and impact, while Trojans and mass mailers continue to rise in frequency and are causing significant damage. We are officially in the Zero Day Era and we expect there will be another big event in 2004 that causes at least a billion dollars in damages. Corporations who do not take adequate time to prepare will be hit hard."

A sample of the findings in the TruSecure research includes:

- In 2004, organizations will see more fast-acting worms like SQL Slammer, Blaster and Nachi that do not use e-mail to attack computers and networks. "These network-aware worms are perimeter killers for organizations. We will also continue to see the impact of mass mailers, especially with home users," says Hughes.
- There will be an increase in Zero Day attacks. "There are so many known and unknown vulnerabilities in Linux, Microsoft, and Internet Explorer that haven't been patched yet," Hughes notes. "Some hacker is going to release exploit code ahead of the patch and create significant damage to those unprepared."
- A significant surge in malware intentionally being posted and unknowingly being shared on P2P file sharing networks. For example, according to new research conducted by Hughes, 45% of the free files collected via KaZaA, the most popular program for downloading free files and music, were viruses, Trojan horse programs and backdoors. "Organizations need to warn their employees about file-sharing applications and the danger they pose to them at work and at home," advises Hughes.

- The emergence of problems associated with "Spyware" piggybacking programs that come with free software. "Spyware" can monitor and track Web wanderings for marketing purposes or even track everything users do on their computers.
- Continued increase in malware that installs open proxies on systems, especially targeting broadband users. The proxy hides the true origin of attacks whether it is viruses, worms or spam. Many of the top viruses in 2003 used tactics like this allowing spammers to send email through these systems.
- On a positive note, TruSecure expects a significant crackdown by the US Government on virus writers. "The government is getting more and more serious and Microsoft is putting out bounties on hackers," Hughes said. "If they catch someone important, like the author of Blaster or SoBig, they are going to make an example and throw the book at the person."

For more information about TruSecure experts or to download the newly-published research, please visit www.TruSecure.com. To arrange an interview with TruSecure experts about the results of the research, please contact Cynthia S. Shaw of TruSecure Corp. at (703) 480-8509 or cshaw@trusecure.com, or Mike Schultz and Laura Ackerman of Schwartz Communications at (781) 684-0770 or TruSecure@schwartz-pr.com.

About TruSecure Corporation

TruSecure is the leading provider of intelligent risk management products and services. TruSecure dramatically improves security and reduces risk by helping organizations make better security decisions and maximize the effectiveness of existing security people, processes, and products. Leveraging TruSecure's vast security knowledge and intelligence gathering resources—including ICSA Labs, the global leader in information security product certification—as well as innovative technology and time-tested processes, our customers can *predict* which vulnerabilities present real risk, *prioritize* remediation efforts, quickly *adapt* to changes in the security threatscape, *measure progress in improving* their security posture, and *document* compliance with applicable security policies, standards and regulations.

Headquartered in Herndon, VA, TruSecure's customer-proven solutions are used by more than 700 customers worldwide, with operations in North America, Central America, Europe and Asia Pacific. For more information about TruSecure Corporation, visit www.TruSecure.com.

Media Contacts

Cynthia Shaw
TruSecure
703-480-8509
PublicRelations@TruSecure.com

ICSA, ICSA Labs and TruSecure are registered trademarks of TruSecure Corporation. All other trademarks and service marks mentioned herein are property of their respective owners.

SLYCK

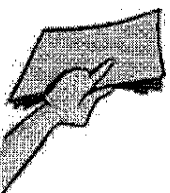
[Home](#) · [Forums](#) · [File-Sharing Dictionary](#) · [Chat](#) · [Contact](#)
[XML RSS Feeds](#)
[Slyck's List of File Sharing Programs and Utilities](#)
[SEARCH SLYCK](#)
[SLYCK GUIDES](#)
[NEW GUIDES](#)
[Xnews](#)
[Agent](#)
[Newsgroups](#)
[Spyware/Adware](#)
[Removal](#)
[TOP GUIDES](#)
[Newsgroups](#)
[Spyware/Adware](#)
[Removal](#)
[All Guides](#)
[WinMX](#)
[FastTrack](#)
[Kazaa Lite](#)
[Kazaa](#)
[iMesh](#)
[Grokster](#)
[eDonkey2K](#)
[eDonkey](#)
[emule](#)
[BitTorrent](#)
[Overnet](#)
[SoulSeek](#)
[IRC](#)
[MP2P](#)
[Piolet](#)
[Blubster](#)
[RocktNet](#)
[DirectConnect](#)
[DirectConnect](#)
[DC++](#)

What's in Your Shared Folder?

July 30, 2004

Thomas Mennecke

The fact that personal information finds its way onto the Internet is nothing new. However, some feel this situation has been exacerbated by the advent of P2P technology. During the installation process, the P2P application asks the end user what folder they would like to share. While more knowledgeable users simply check off a specific folder, many other inexperienced users share their entire root directory (AKA the "C:" directory.)



Sound like a problem? Perhaps not to the average P2Per, who may simply peruse unwittingly shared documents for their entertainment value. When it comes to shared personal information, the most prolific network seems to be Gnutella. Last night I dusted off BearShare and fired the Gnutella client up. I went to the options menu, checked off the file extension option and went to work. To start off, I used "*.doc" and "*.xls" as search queries. These extensions are associated with Microsoft Word documents and Excel spreadsheets.

Within seconds, the search results started to pour in. Some files existed with the intent to be shared, such as e-books and program serials. However, others fell into the category of carelessness and utter disregard for ones sharing practices. These files included résumés, bank account information, credit card statements, letters of all kinds, book reports, children's homework and a household chore schedule. Let us take a sample of one of these résumés below:

Jodyne L.

Gnutella
Shareaza
Gnucleus
XoloX
LimeWire
BearShare
Morpheus

ARCHIVE

November
October
September
August
July
June

Search The Archive:

Objective

To obtain a full-time Account Manager position with [redacted] in [redacted], WI

Education

Bachelor of Business Administration • University of [redacted] • May 2004 • Marketing, emphasis in promotion • Minor in Management • Advanced Business Communications Certificate • Cumulative GPA: 3.34, Major GPA: 3.21.

Key Skills

Market research • online research • written and oral communication • telephone • customer service • typing • 10-key calculator • Microsoft Word, Excel, PowerPoint and Publisher • Dreamweaver • SPSS • Adobe Photoshop • organization • innovative thinking • leadership • team work • dedication • promptness • responsibility • friendly • entrepreneurial • time management • human resources • financial services • management training • cross-selling • self-motivated

Work Experience

Production Assistant • University Printing Services • [redacted] • August 2001-Present
 ▶ Completed orders for customers; padded, cut, bound, folded, shelved, delivered orders

Jodie may have good Photoshop skills, but she doesn't know the first thing about file-sharing.

With this information, we know she is applying for a job with XYZ Corporation, and we also know her full name, address, and home phone number. A less scrupulous person would be able to fully take advantage of this individual, perhaps giving her a call and making an offer of \$100,000 a year salary just for kicks. And that is the same concern that Glen from SeeWhatYouShare.com is focusing on.

However, Glen has also noted something perhaps more sinister than simply a few bank statements and résumés shared on the Gnutella network. From simply scanning for Word documents, Glen has come across various military personnel memos, many including soldiers

Ads by Google

P2P File Sharing Software

Enjoy unlimited access to Movies, Music, Software, Games & more!
www.247downloads.com

Songs - Free Downloads

12 Billion Songs, No Download Fees
 100% Free & Legal Music Downloads!
iMusicSearch.com

Looking For Legal P2P?

Get Legal for Only \$19.95. Compare MP3Advance, K-Lite, DCMoviez, etc.
www.FileShareSoftware.com

Secure File Sharing

Share files securely with friends & colleagues with Mirra
www.mirra.com

name and social security numbers. This is information that should obviously be confidential. While Greg does not advocate the stoppage of P2P in any way, his intention is to bring greater attention to the growing trend of lacks sharing practices.

"Many people who use P2P software do not understand it, and as a result, they end up sharing everything. This is critical especially for individuals who do office work on their personal computers (since you are not supposed to install software on your work computer). Also, it is critical as military members take their personal computers into a theater of operations and then return from those areas without removing sensitive information from their hard drives. My intent with this site is not to have P2P stopped. It will never happen. However, I would like users of P2P applications to intentionally select what files they want to share, and end the scanning of hard drives for shareable files. The "click yes" installation for some P2P applications results in sharing everything with certain extensions (.doc, .ppt, .pps, .xls, .rtf, .tif, .mp3, .mpg, etc.) even if they are not in any shared folder, which ultimately results in a complete loss of privacy for many P2P users."

"The software engineers need to rethink the way their software misleads the users of their products. Do you read the fine print from top to bottom on every piece of software you install on your computer? The default installation should be, in my opinion share nothing and once you are confident in what you are doing the end user would then be able to select files for sharing, of course knowing the consequences for the files they select. I do not believe the massive leaks from the military standpoint would exist had the end user known what the P2P application was doing in the background."

File-sharing developers are listening to what sites like SeeWhatYouShare.com have to say, however their approach to a resolution is much more tempered. Ultimately, the end user is responsible for their own actions, and need to recognize they are using a file-sharing application. The implications of using a file-sharing application carry a certain degree of responsibility, as Greg Bildson, COO of LimeWire, explains.

"We have been looking at addressing the accidental sharing issue for a while. Certainly, more can be done to warn users when they are about to share large numbers of files. One common complaint that we do avoid is that we don't have a "Shared" folder on the users desktop. Applications that use those types of shortcuts can allow users to accidentally drop files on their shared folder and have those files shared without their knowledge.

That being said, these are file sharing applications. The main goal of a file sharing application is to make it easy for users to share files. Users need to be aware of what they are doing. For those users that don't know what they are doing, file sharing applications need to be a little more bulletproof.

Given that file sharing is still a relatively new type of application, it makes sense that the developers have not worked out all of the security issues. We are still focused on improving the P2P protocol."

BearShare and LimeWire, the two main forces behind Gnutella, are acutely aware of the situation and are actively working to resolve it. BearShare in fact has "locks" on the "C:" and "Program Files" directories, preventing any accidental sharing. While this may seem like an urgent issue, there is much more smoke than there is fire. With more vigilance on the part of individuals, P2P developers, and sites like SeeWhatYouShare.com, this is a problem that will eventually correct itself.

You can discuss this article here - 46 replies

Sponsored Links:
Algebra Help

Home | Contact
©2001-2004 slyck.com

P2P On Government Computers – Orders and Concerns

Federal

Office of Management and Budget (OMB)

Memorandum on “Personal Use Policies and ‘File Sharing’ Technology,” 9/8/04
(<http://www.whitehouse.gov/omb/memoranda/fy04/m04-26.html>)

Order

- “Agencies’ IT security or ethics training must train employees on agency personal use policies and the prohibited improper uses of file sharing.”
- “Operational controls detailing procedures for handling and distributing information and management controls outlining rules of behavior for the user must ensure the proper controls are in place to prevent and detect improper file sharing.”

Warning

- “While there are many appropriate uses of this technology, a number of studies show, the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggests P2P is a common avenue for the spread of computer viruses within IT systems.”

FY2004 Reporting Instructions for the Federal Information Security Management Act,
8/23/04

(<http://csrc.nist.gov/sec-cert/m04-25.pdf>)

Order

- “Federal computer systems, as well as those operated by contractors on the government’s behalf, must not be used for the downloading of illegal and/or unauthorized copyrighted content, including illegal downloads using file sharing programs.”

Warning

- “While there are many appropriate uses of this technology, a number of studies show, the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggests P2P is a common avenue for the spread of computer viruses within IT systems.”

U.S. Department of Agriculture

“Interim Guidance on Peer-to-Peer Software and Copyright”
(<http://www.usda.gov/da/IRD/CS-010.htm>)

Order

- “USDA agency Internet Protocol (IP) addresses, particularly in the Washington DC area, have been identified engaging in the illegal download of software, music, graphics, or videos that are protected by copyright laws or in some instances, pornography.”

- “These ‘evasive’ programs...have no recognized business need and should not be loaded on workstations/equipment used to conduct USDA Official Business.”

Warning

- “These ‘evasive’ programs are used for illegal activity, such as pornography and software piracy, and have the ability to send inbound and outbound traffic to regular Internet ports for transport, thus disguising their purpose. They have no recognized business need and should not be loaded on workstations/equipment used to conduct USDA Official Business.”
- “Efforts to remove these programs can involve days of effort rebuilding the device causing undue departmental expense. Repeated and continuous use of this type software can impact network resources and inhibit USDA’s ability to properly perform our mission. In addition, if USDA does not control copyright violations of video, software, music and graphics, we may be subject to prosecution in lieu of the actual offender.”

U.S. Department of Commerce

Memorandum on “Commerce IT Security Policy on Peer-to-Peer File Sharing,” 5/21/04
(http://www.osec.doc.gov/cio/oipr/ITSec/p2p_policy.htm)

Order

- “Commerce prohibits unauthorized P2P file sharing technology from use on Commerce IT systems unless it has been explicitly authorized in writing by an operating unit CIO in support of an official Commerce IT application.”

Warning

- “P2P technology, when misused, can lead to possible copyright infringement or the appearance of copyright infringement by employees. It may even appear that an entire organization is culpable, unless special attention has been given by the organization to preventing such actions. The use of public P2P technology is potentially much worse than a user simply downloading files from a system somewhere on the Internet. Users of P2P technology may (even unknowingly or unintentionally) be supporting file sharing by others due to the capabilities of the downloaded public P2P software. There are significant additional IT security risks associated with public P2P technology.... These concerns are in addition to loss of employee productivity by downloading and listening to or watching the content of such files and the use of Government network and computing resources while doing so.”
- “The Department of Justice told the Federal CIO Council that ‘...The vast majority of files that are traded on P2P networks are copyrighted music files.’”
- “In addition, the Department of Justice informed us that many of the software packages downloaded by users to support their involvement in sharing files using public P2P technology can also be set up to make files

on a user's computer accessible to large numbers of people on the Internet. Some of these files, if they have been copied from other users' systems on the Internet using P2P technology, may represent copyright infringement or the appearance of copyright infringement. Making them available on a Commerce computer for copying by users on the Internet may also result in copyright infringement. In addition, people who use P2P technology not only may be sharing music and other files illegitimately over the Internet but also inadvertently sharing the entire contents of the hard drive on their computer."

U.S. Department of Justice

Memorandum on "Use of Peer-to-Peer File Sharing Technology," 9/17/04

Order

- "Department computer systems, as well as those operated by contractors on the Government's behalf, may not be used for the sharing of illegal material or unauthorized copyrighted material. There are very rare occasions when employees need to use P2P capabilities within the Department. Such uses can only be authorized after consultation with the CIO. Use of the P2P file sharing using the internet is expressly forbidden. Technical controls on such use are already in place and they will be strengthened as appropriate." (emphasis added)

Warning

- "While there are many appropriate uses of this technology, research shows that the vast majority of files exchanged on P2P networks are copyrighted music, motion pictures, and pornography. P2P file exchanges are also a common distribution avenue for viruses and other types of malicious code."

U.S. Army

"Downloading shared files threatens security," Army News Service, 4/22/04 (http://www4.army.mil/ocpa/print.php?story_id_key=5878)

Order

- "The Army's regulation on Information Assurance, Army Regulation 25-2, specifically prohibits certain activities; sharing files by means of P2P applications being one of them."

Warning

- "In a white paper written by the Army's Computer Network Operations Intelligence section, unauthorized P2P applications on government systems, 'represent a threat to network security.'"
- "'The idea of someone else getting unfettered access to anything of yours without your explicit consent should scare anybody – and that's exactly what P2P authorizes,' says Zina Justiniano, an intelligence analyst with the U.S. Army Network Enterprise Technology Command's (NETCOM) Intelligence Division, G2. 'P2P is freeware. ... The fact that it's free says

that anybody and their cousin can get it; that means that anybody and their cousin can get to your machine.”

- “P2P applications are configured to use specific ports to communicate within the file sharing ‘network,’ sometimes sidestepping firewalls. This circumvention creates a compromise and potential vulnerabilities in the network that, in a worse case scenario, can lead to network intrusions, data compromise, or the introduction of illegal material and pornography.”
- “There are several known Trojan horses, worms and viruses that use commercial P2P networks to spread and create more opportunities for hackers to attack systems.”

State

California—Executive Order S-16-04

(http://www.governor.ca.gov/state/govsite/gov_htmldisplay.jsp?sFilePath=/govsite/executive_orders/20040917_S-16-04.html&sCatTitle=Executive%20Orders&iOID=58763&sTitle=Executive%20Orders%20%20%20&BV_SessionID=@@@@1930992695.1099433525@@@@&BV_EngineID=cccjadcmnghjhgicfngcfkmdffidfog.0)

Order

- “The State Chief Information Officer shall develop a statewide policy for use by each state agency, department, board, commission and office of the executive branch regarding the use of peer-to-peer file-sharing programs on state computers, including a prohibition of such programs that pose risks to the security and integrity of state computer systems.”

Warning

- “...the presence of certain peer-to-peer file-sharing software on state computers presents a significant security risk by potentially allowing individuals outside of the state system to access confidential and sensitive information that may be stored or maintained on state computers and networks”
- “...use of some peer-to-peer file-sharing services on state government computers and networks can threaten the security and privacy of the information on those computers”
- “...some peer-to-peer file-sharing services may permit viruses and other malicious programs to gain access to state computer systems”
- “...use of some peer-to-peer file-sharing services consumes network resources, which may reduce the performance of state computer systems and impact the state's ability to effectively function and provide efficient services to the public”
- “...currently peer-to-peer file-sharing services are often used to enable illegal dissemination and downloading of copyrighted material, including music, motion pictures, software and video games, resulting in huge losses of revenue to the state's valuable entertainment industry”

Maryland—“Governor pushed for file sharing warning,” The Diamondback, 1/30/04

(<http://www.inform.umd.edu/News/Diamondback/archives/2004/01/30/news5.html>)

Order

- “A memorandum released to students, faculty and staff ... about the dangers of peer-to-peer file sharing was influenced by concerns from Gov. Bob Ehrlich’s office about illegal downloading on state-owned networks.”

Warning

- “The letter, written by Provost Bill Destler and Mark Henderson, Office of Information Technology interim vice president and chief information officer, warned the university community about the possibility of criminal prosecution and the consequences of downloading copyrighted music and movies.”
- “Representatives from Ehrlich's office met with university officials over the past two months to discuss the problems of file sharing on the campus.”

Michigan—“Traffic to block outbound to the Internet”

http://www.michigan.gov/documents/Internet_Block_Traffic_86990_7.pdf

Order

- “outbound Internet access for the applications/services below will be restricted... Peer-to-peer File Sharaing:”

Warning

- “The applications/services...are not known to support the State’s business, invite unacceptable use by employees, and greatly increase risk to the State’s network.”

May 21, 2004

MEMORANDUM FOR: Heads of Operating Units
Chief Information Officers

FROM: Thomas N. Pyke, Jr.

SUBJECT: Commerce IT Security Policy on Peer-to-Peer File Sharing

What is P2P technology?

What is the Commerce Policy Regarding P2P?

Why is the Department of Commerce concerned about P2P technology?

How does this addendum relate to existing Commerce IT Security and Internet Use Policies?

What should Commerce operating units do to address the Department's concerns with P2P technology?

Addendum to the Department of Commerce IT Security Policy Restrictions on the Use of Peer-to-Peer (P2P) File Sharing

Recent increased public concern about unauthorized use of Government computers, including use of public peer-to-peer (P2P) technology, coupled with reports of possible unauthorized use of Government computers involving P2P technology in two of our Operating Units, led to this IT Security policy addendum. This addendum includes standards and controls for determining unauthorized use, prevention of unauthorized use, and monitoring for unauthorized use. Enforcement of this policy is effective immediately.

What is P2P technology?

P2P technology refers to any software or system that allows individual users of the Internet to connect (directly, through the Internet) to each other so as to transfer or exchange computer files. The definition used by the Federal Enterprise Architecture is that P2P technology is a class of applications that operates outside the Internet Domain Name Service (DNS) system, that has significant or total autonomy from central servers, and that takes advantage of resources available on the Internet.

What is the Commerce policy regarding P2P technology?

The attached addendum to the *Commerce IT Security Program Policy* states that Commerce prohibits unauthorized P2P file sharing technology from use on Commerce IT systems unless it has been explicitly authorized in writing by an operating unit CIO in support of an official Commerce IT application.

Why is the Department of Commerce concerned about P2P technology?

P2P technology, when misused, can lead to possible copyright infringement or the appearance of copyright infringement by employees. It may even appear that an entire organization is culpable, unless special attention has been given by the organization to preventing such actions. The use of public P2P technology is potentially much worse than a user simply downloading files from a system somewhere on the Internet. Users of P2P technology may (even unknowingly or unintentionally) be supporting file sharing by others due to the capabilities of the downloaded public P2P software. There are significant additional IT security risks associated with public P2P technology, as noted below. These concerns are in addition to loss of employee productivity by downloading and listening to or watching the content of such files and the use of Government network and computing resources while doing so.

The Department of Justice told the Federal CIO Council that "such systems are highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. The vast majority of files that are traded on P2P networks are copyrighted music files." The use of publicly available P2P software for purposes such as this is referred to as "public" P2P technology.

In addition, the Department of Justice informed us that many of the software packages downloaded by users to support their involvement in sharing files using public P2P technology can also be set up to make files on a user's computer accessible to large numbers of people on the Internet. Some of these files, if they have been copied from other users' systems on the Internet using P2P technology, may represent copyright infringement or the appearance of copyright infringement. Making them available on a Commerce computer for copying by users on the Internet may also result in copyright infringement. In addition, people who use P2P technology not only may be sharing music and other files illegitimately over the Internet but also inadvertently sharing the entire contents of the hard drive on their computer.

How does this addendum relate to existing Commerce IT Security and Internet Use Policies?

The addendum complements the existing Commerce *IT Security Program Policy* and the *Internet Use Policy*, which define employee responsibilities, authorized use of Commerce IT systems, and outline the management, operational, and technical control minimum standards to protect Commerce systems. These policies include the following sound IT security practices and may help prevent unauthorized use of P2P technology:

Operating Unit Heads must ensure that the operating unit has an established IT Security Program and ensure adequate resources are provided to implement IT security activities. The program must include mechanisms to educate Commerce personnel regarding IT security policies and procedures and must address the consequences of policy violations, such as those imposed under Department Administrative Order 202-751, *Discipline* (found at <http://www.osec.doc.gov/omo/daos/202-751.htm>).

Program Officials must support the process of system accreditation, which verifies and validates the adequacy of system security controls, and authorize systems to operate in support of the Commerce mission.

System Owners must develop system security plans that address adequate system security measures, to include:

- Establishing rules of behavior for system users, including remote users.
- Configuring firewalls that protect systems on Commerce internal networks to close ports not required for official Commerce IT applications. Through an established system configuration management process (ideally including a review by the operating unit IT security office), the system owner must approve port use in writing (with the exception of ports 80 and 443).
- Configuring network devices such as firewalls, routers, and intrusion detection systems to filter incoming and outgoing traffic such as unauthorized P2P transmissions that may be port-sensitive.
- Monitoring network performance.
- Logging unusual activity and attempts of P2P transmissions where they can be detected.
- Supporting the enforcement of consequences for unauthorized use of P2P technology by Commerce personnel.
- Ensuring certification testing of all system controls to validate their effectiveness and ensuring accreditation of systems to establish accountability for system security.

The Commerce *IT Security Program Policy and Minimum Implementation Standards (IT Security Policy)* can be viewed on the Web at

<http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm>

All personnel (including federal employees, contractors, guest researchers, collaborators, and others) are expected to comply with published rules for ethical behavior and for acceptable system use, including those established by the Commerce *Internet Use Policy* (found at http://home.commerce.gov/Internet_use_policy.htm). In addition, the recently issued, revised Commerce Internet Use Policy prohibits 1) Internet use that could generate or result in an additional charge or expense to the Government and 2) participation in or encouragement of illegal activities or the intentional creation, downloading, viewing, storage, copying, or transmission of illegal or discriminatory materials.

What should Commerce operating units do to address the Department's concerns with P2P technology?

Please review your operating unit policies and procedures to ensure they are aligned with this policy addendum. If you have questions, please contact Nancy DeFrancesco, the Department's IT Security Program Manager, at (202) 482-3490.

**Addendum to the Department of Commerce IT Security Policy
Restrictions on the Use of Peer-to-Peer (P2P) File Sharing**

This addendum to the Commerce *IT Security Program Policy* applies to all classified national security and unclassified Commerce systems used to process and store Commerce information, and to all Commerce operating units and personnel (federal and contractor), guest researchers, collaborators, and others requiring access to the hardware and software components of any Commerce IT systems. It also requires implementation of specific controls to protect Commerce IT systems from compromise, as well as controls to prevent, detect, and respond to unauthorized activity. The following policy statement and the specified minimum standards and controls are intended to prevent and detect unauthorized use of Peer-to-Peer (P2P) technology.

The Department prohibits use of P2P file sharing technology on any Commerce IT system unless it has been explicitly authorized in writing by an operating unit CIO in support of an official Commerce IT application. A copy of each such authorization shall be sent to the Commerce CIO. In implementing this policy, CIOs must give special attention to ensuring that public P2P technology is not being used to support sharing of computer files that contain music, digital film, TV shows or other information such that copying of the files may infringe on any copyrights or other associated intellectual property restrictions.

Operating unit CIOs shall be especially careful that any of the following public online file-sharing services, or similar services, designed to facilitate the sharing of computer files (including music, digital film, and TV shows) are not used on any Commerce IT system in such a way as to potentially infringe on copyrighted material:

1stWorks, AudioFind, BadBlue, BearShare, Blubster, CareScience, Clip2, DirectConnect, FastTrack, Fatbubble, File Rogue, Filetopia, FreeWire, Frontcode Technologies, FurthurNet, Gnotella, Gnutella, Grokster, Harmonic Invention Software, Hotline Connect, iMesh, Ionize, Jibe, Jungle Monkey, KaZaA, LimeWire, MangoSoft, Morpheus, Myster, NextPage, Inc., Ogg Vorbis, Ohaha, OnSystems, OpenNap, Pointera, Radio Userland, Rapigator, Shareaza, Softwax, Songbird, SongSpy, Spinfrenzy.com, Splooge, Streamcast, Swaptor, Thinkstream, Toadnode.com, LLC, Tripnosis, Inc., Vitaminic, WebDAV.

Commerce CIOs should ensure that system owners uninstall unauthorized P2P software and that they implement adequate controls to prevent it from being installed and used on Commerce computers, including use of administrative and technical means to:

- Limit the ability of Commerce internal network users to load software themselves on computers. This control concept can be supported by the use of automated software patching tools and centralized oversight of large numbers of computers in an automated manner, while maintaining tight configuration control over all computers.
- Evaluate and implement cost-effective mechanisms to monitor and detect unauthorized P2P activity within Commerce networks.
- Communicate P2P awareness information to internal network users and to remote users (such as teleworkers and researchers processing and storing Commerce data on personally-owned computers).

This addendum to the Commerce *IT Security Program Policy* is authorized by Tom Pyke, Commerce CIO, is effective on May 21, 2004, and will remain in effect until incorporated into the next update of the Commerce *IT Security Program Policy*.



THE DIRECTOR

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-04-25

August 23, 2004

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten 
Director

SUBJECT: FY 2004 Reporting Instructions for the Federal Information Security Management Act

This memorandum provides updated instructions for agency reporting under the Federal Information Security Management Act of 2002 (FISMA). Agency Chief Information Officers and Inspectors General have also received a copy of the attached instructions.

FISMA provides the framework for securing the Federal government's information technology. All agencies covered by the Paperwork Reduction Act must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB) and Congress on the effectiveness of their security programs. The reports must also include independent evaluations by the agency Inspector General.

Agencies are to transmit their FY04 reports to OMB by October 6, 2004. Guidance for transmitting the reports to Congress is set out in the attached instructions.

OMB uses the reports to help evaluate government-wide security performance, develop its annual security report to Congress, assist in improving and maintaining adequate agency security performance, and inform development of the E-Government Scorecard under the President's Management Agenda.

In addition to the formal report transmittal to OMB, an electronic copy of the report should also be sent to Kristy LaLonde at klalonde@omb.eop.gov and Daniel Costello at daniel_j_costello@omb.eop.gov. Please contact Glenn Schlarman at 202-395-4951 if you have any questions.

We appreciate your ongoing efforts in addressing this critical issue and for completing these reports in an accurate and timely manner.

Attachments

What is the link between the E-Authentication Risk Assessment and the FISMA Risk Assessment and Certification and Accreditation Security Requirements?

The E-Authentication Guidance for Federal Agencies established the requirement that agencies conduct an e-authentication risk assessment on those systems that remotely authenticate users over a network for purposes of e-government and commerce.

On December 16, 2003 OMB issued M-04-04, "E-Authentication Guidance for Federal Agencies." As stated in M-04-04, agencies must categorize all existing transactions/systems requiring user authentication into one of the described assurance levels by September 15, 2005. Agencies should accomplish this in the following order:

- Systems categorized as "major" must be completed by December 15, 2004.
- New authentication systems should begin to be categorized, as part of the system design on September 24, 2004. This is 90 days following the completion of the final E-Authentication Technical Guidance issued by NIST. NIST Special Publication 800-63 "Recommendation for Electronic Authentication" is available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf.

This risk assessment should be conducted in parallel with the overall system risk assessment and in the context of greater policy issues, and should be conducted with the advice of agency legal, policy, privacy, and agency business process owners. Additionally, agencies should address the requirements of M-04-04 in their System Security Plans and certify the requirements prior to authorization to process.

Why is OMB asking about Peer to Peer file sharing in IT security training?

IT security awareness training should evolve as emerging technologies enter into the workplace. A type of file sharing (known as Peer to Peer or P2P) generally refers to any software or system allowing individual users of the Internet to connect to each other and trade computer files. These systems are usually highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. While there are many appropriate uses of this technology, a number of studies show the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggests P2P is a common avenue for the spread of computer viruses within IT systems.

Federal computer systems, as well as those operated by contractors on the government's behalf, must not be used for the downloading of illegal and/or unauthorized copyrighted content, including illegal downloads using file sharing programs. Further information is detailed in the Chief Information Officers Council's recommended guidance on "Limited Personal Use of Government Office Equipment Including Information Technology⁴". OMB expects agency policies and training programs to be consistent with the CIO Council guidance.

⁴ http://www.cio.gov/documents/peruse_model_may_1999.pdf (May 19, 1999)

USDA UNITED STATES DEPARTMENT OF
AGRICULTURE
Office of Operations
Information Resources Division

TO: Agency Chief Information Officers

FROM: William Hadesty
Associate Chief Information Officer
Office of Cyber Security

SUBJECT: Interim Guidance on Peer-to-Peer Software and Copyright
Protection, CS-010

The Office of Cyber Security is in an evolutionary process of improving USDA's Intrusion Detection sensors and firewalls around the country. In this regard, we have been intensely scanning our systems to detect virus programs, worms or intrusions in our IT systems. During this process, we have been detecting increased activity in areas that all users should know are inappropriate.

USDA agency Internet Protocol (IP) addresses, particularly in the Washington DC area, have been identified engaging in the illegal download of software, music, graphics, or videos that are protected by copyright laws or in some instances, pornography. These addresses are using a number of "Peer to Peer" software & "file sharing" products that are available for download from the Internet. Some of the products that we have detected are: gnutella, LimeWire, SwapNut, KaZaA, MORPHEUS and all similar P2P software.

These "evasive" programs are used for illegal activity, such as pornography and software piracy, and have the ability to send inbound and outbound traffic to regular Internet ports for transport, thus disguising their purpose. They have no recognized business need and should not be loaded on workstations/equipment used to conduct USDA Official Business.

Efforts to remove these programs can involve days of effort rebuilding the device causing undue departmental expense. Repeated and continuous use of this type software can impact network resources and inhibit USDA's ability to properly perform our mission. In addition, if USDA does not control copyright violations of video, software, music and graphics, we may be subject to prosecution in lieu of the actual offender.

USDA has a long established policy that it does not condone or support employees who use Government computers and networks in an inappropriate manner. The Limited

Personal Use Policy cannot be used as a justification for illegal or inappropriate use and practices. All USDA contractors need to be advised that they are subject to compliance with all Federal laws and USDA regulations when they and/or their company is receiving USDA funds for services they are performing on behalf of USDA. Use of non-USDA, non-Federal computers, including laptops, does not exempt the contractor from USDA and Federal laws.

The Office of Cyber Security will continue to take aggressive measures to combat this unacceptable practice to include: forwarding all instances of pornography to OIG, any child pornography detected in our scans will be referred to the appropriate U. S. Attorney's office and to recommend appropriate administrative action be taken

against employees/contractors violating this policy. All agencies and staff offices will enforce their responsibilities to protect USDA Information Technology Resources from misuse, inappropriate and illegal activity. Your users should be advised that they are personally responsible for all costs related to trafficking in music, software or videos if a complaint is filed against them and the copyright owner seeks restitution of funds lost due to pirating copyright protected material. The cost for each occurrence, plus recovery costs, are assessed to the offending party. Further, each agency will monitor their employees and contractors to ensure that they adhere to the requirements of this policy in conducting Official USDA business.

The Office of Cyber Security is actively pursuing legal remedies to stop these activities and will be publishing further guidance in these areas in the coming months. Please review this draft Interim Guidance and provide your comments to Sharon Hughes within 30 days from issuance of this memorandum. If you have questions or concerns, please contact me directly on (202) 690-0048 or by E-mail at bill.hadesty@usda.gov.

CS Staff Members

Agency ISSPMs

[United States Department of Agriculture](#) | [Departmental Administration](#) | [About OO](#)

We welcome comments and suggestions about this website. Please direct them to [DAWebmaster](#)

[USDA Privacy Policy](#) | [Accessibility Statement](#)



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-04-26

September 8, 2004

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM:

Karen S. Evans 
Administrator, IT and E-Gov

SUBJECT:

Personal Use Policies and "File Sharing" Technology

The purpose of this memorandum is to detail specific actions agencies must take to ensure the appropriate use of certain technologies used for file sharing across networks. These actions are based on recommended guidance developed by the CIO Council in 1999. The effective use and management of file sharing technology requires a clear policy, training of employees on the policy, and monitoring and enforcement.

Background

A type of file sharing known as Peer-to-Peer (P2P) refers to any software or system allowing individual users of the Internet to connect to each other and trade files. These systems are usually highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. While there are many appropriate uses of this technology, a number of studies show, the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggests P2P is a common avenue for the spread of computer viruses within IT systems.

Federal computer systems or networks (as well as those operated by contractors on the government's behalf) must not be used for the downloading of illegal and/or unauthorized copyrighted content. It is important to ensure computer resources of the Federal government are not compromised and to demonstrate to the American public the importance of adopting ethical and responsible practices on the Internet.

The CIO Council has issued recommended guidance on "Limited Personal Use of Government Office Equipment Including Information Technology.¹" Examples of inappropriate personal use include "the creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited" and "the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data."

¹ http://www.cio.gov/documents/peruse_model_may_1999.pdf (May 19, 1999)

Direction to Agencies

Effective use and management of file sharing technology requires a clear policy, training of employees on the policy, and monitoring and enforcement. Specifically, agencies are directed to:

1. Establish or Update Agency Personal Use Policies to be Consistent with CIO Council Recommended Guidance.

OMB expects all agencies to establish personal use policies, consistent with the recommended guidance developed by the CIO Council. Agencies who have not established personal use guidance should do without delay, but no later than December 1, 2004.

2. Train All Employees on Personal Use Policies and Improper Uses of File Sharing

Agencies' IT security or ethics training must train employees on agency personal use policies and the prohibited improper uses of file sharing. Training must be consistent with OMB Circular A-130, appendix III paragraph (3)(a)(b) which states agencies must "ensure that all individuals are appropriately trained in how to fulfill their security responsibilities [...]. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques."

On October 6, 2004, as part of the agency annual reports required by Federal Information Security Management Act of 2002 (FISMA) described in OMB Memorandum 04-25, FY 2004 Reporting Instructions for FISMA2 agencies must report whether they provide training regarding the appropriate use of P2P file sharing.

3. Implement Security Controls to Prevent and Detect Improper File Sharing

As required by FISMA, agencies are to use existing NIST standards and guidance to complete system risk and impact assessments in developing security plans and authorizing systems for operation. Operational controls detailing procedures for handling and distributing information and management controls outlining rules of behavior for the user must ensure the proper controls are in place to prevent and detect improper file sharing.

Again, OMB recognizes there are appropriate uses of file sharing technologies, but as with all technology it must be appropriately managed.

If you have any questions regarding this memorandum, please contact Jeanette Thornton, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3562, fax (202) 395-5167, e-mail: jthornto@omb.eop.gov.




U.S. Department of Justice

Washington, D.C. 20530

September 17, 2004

MEMORANDUM FOR HEADS OF COMPONENTS
COMPONENT CHIEF INFORMATION OFFICERS
ALL DEPARTMENT OF JUSTICE EMPLOYEES

FROM: Paul R. Corts 
Assistant Attorney General for Administration

SUBJECT: Information Technology Security Awareness Training
Use of Peer-to-Peer File Sharing Technology

Peer-to-Peer (P2P) file sharing is a capability that allows individual users of the Internet to connect to each other and share files. These systems tend to be highly decentralized and tailored to persons seeking to exchange certain types of files. While there may be appropriate uses of this technology, research shows that the vast majority of files exchanged on P2P networks are copyrighted music, motion pictures, and pornography. P2P file exchanges are also a common distribution avenue for viruses and other types of malicious code.

Department computer systems, as well as those operated by contractors on the Government's behalf, may not be used for the sharing of illegal material or unauthorized copyrighted material. There are very rare occasions when employees need to use P2P capabilities within the Department. Such uses can only be authorized after consultation with the CIO. Use of the P2P file sharing using the Internet is expressly forbidden. Technical controls on such use are already in place and they will be strengthened as appropriate.

Every component in the Department of Justice is anxious to use new information technology (IT) to service our mission. At the same time, we must continuously monitor our systems and networks and the use of new technology to ensure the integrity, confidentiality, and availability of IT services.

This memo is intended to augment IT security training for all users by increasing your awareness of the vulnerabilities and policies associated with P2P. Training material on P2P file sharing will be included in online security awareness training programs used in the Department. If you have any questions or require additional information on P2P, please contact Martin Burkhouse on (202) 616-4574, or by email at martin.t.burkhouse@usdoj.gov.



Downloading shared files threatens security

By Sgt. 1st Class Eric Hortin
April 22, 2004

FORT HUACHUCA, Ariz. (Army News Service, April 22, 2004) – People spend hours in front of their computer screen, downloading music or new movies from the Internet, and not paying a cent, the Army considers such action on government computers to be a security threat.

One program that is used to download files is Peer-to-Peer (P2P) architecture. It is a type of network in which each workstation has the capability to function as both a client and a server. It allows any computer running specific applications to share files and access devices with any other computer running on the same network without the need for a separate server. Most P2P applications allow the user to configure the sharing of specific directories, drives or devices.

In a white paper written by the Army's Computer Network Operations Intelligence section, unauthorized P2P applications on government systems, "represent a threat to network security."

"The idea of someone else getting unfettered access to anything of yours without your explicit consent should scare anybody – and that's exactly what P2P authorizes," says Zina Justiniano, an intelligence analyst with the U.S. Army Network Enterprise Technology Command's (NETCOM) Intelligence Division, G2. "P2P is freeware. Freeware, shareware – most of the stuff that you pay nothing for, has a high price. The fact that it's free says that anybody and their cousin can get it; that means that anybody and their cousin can get to your machine."

P2P applications are configured to use specific ports to communicate within the file sharing "network," sometimes sidestepping firewalls. This circumvention creates a compromise and potential vulnerabilities in the network that, in a worse case scenario, can lead to network intrusions, data compromise, or the introduction of illegal material and pornography.

There is also the issue of bandwidth. Since the start of the global war on terrorism, the most pressing issue from service members in the field has been the shortage of bandwidth to transmit battlefield intelligence to combatant commanders. The average four-minute song converted into an audio file recorded at 128-bit, can be upwards of 5 megabytes. Full-length video MPEG files can easily reach 1.6 gigabytes. Depending on the connection speed, even a small file may take several minutes to hours to download, using valuable bandwidth.

Unauthorized use of P2P applications account for significant bandwidth consumption. It limits the bandwidth required for official business, and storage capacity on government systems.

While those who monitor the Army networks agree that copyright infringement is a valid issue, they do have other, more important concerns.

There are several known Trojan horses, worms and viruses that use commercial P2P networks to spread and create more opportunities for hackers to attack systems. Trojan horse applications record information and transmit it to an outside source. They can also install “backdoors” on operating systems, transmit credit card numbers and passwords – making these malicious programs a favorite of hackers. Some of the malicious codes allow hackers to snoop for passwords, disables antivirus and firewall software, and links the infected system to P2P networks to send large amounts of information (spam) using vulnerabilities in Windows operating systems.

“If it’s a really good Trojan horse, it will actually run two programs; it will run the program they said they were going to run, so they will not only download it, but they will install it and be very happy that it’s there,” Justiniano said. “Meanwhile in the background, another program is doing malicious damage to the computer by either damaging files or possibly taking files off the computer without your knowledge. If it’s a really nice program that runs well, (the user) will pass that file over to someone else because they really got their money’s worth out of it. People will just keep passing it along.”

Trojan horses are not the cause of all security issues. Oftentimes, “spyware” applications are installed with the users consent; it’s buried in the really long agreement that nobody reads that a user must click, “I Accept,” in order to begin the installation. This is especially true with free-ware applications downloaded from the Internet. According to published reports, a couple of years ago, some P2P applications came packaged with a spyware application that acted as a Trojan horse. This specific program sent information to an online lottery server.

Those are just a couple of reasons the Army doesn’t want its people loading P2P on their systems, and enacted regulations prohibiting loading those applications.

The Army’s regulation on Information Assurance, Army Regulation 25-2, specifically prohibits certain activities; sharing files by means of P2P applications being one of them. There are some, however, who have P2P applications on their Army systems and use them despite the prohibition of such activities.

Over a two-month period at the end of last year, government organizations identified more than 420 suspected P2P sessions on Army systems in more than 30 locations around the globe.

It seems some don’t understand or haven’t read the standard Department of Defense warning that says, “Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring.” For those who think, “How are they going to know it’s me? I’m just one person in a network of hundreds of thousands,” don’t be surprised when network access is cut off and the brigade commander is calling.

It is the role of the Theater Network Operations and Security Center, located in Fort Huachuca, Ariz., to monitor and defend its portion of the Army network. This includes identifying potential security risks to the network, and unauthorized P2P applications, which create a considerable risk to those networks.

“People shouldn’t assume they are using P2P applications in secrecy,” said Ronald Stewart, deputy director of the C-TNOSC. “We are able to detect use of P2P, and when we do, we take measures. We can detect and identify systems with P2P software on them; and when we find them, we direct the removal of the software from the system through the command chain.”

Some Soldiers try to work around the Army networks to feed their P2P habits. Lt. Col. Roberto

Andujar, director of the C-TNOSC, says using the Terminal Server Access Controller System (TSACS) to dial into the military network is not a work-around, because there are tools in place to identify P2P traffic.

Methods commonly used by commercial industry, such as Internet Protocol (IP) address and port blocking, random monitoring, and configuring routers are some of the methods the C-TNOSC and installations take to prevent P2P access. There are other methods used, but specific examples cannot be discussed.

Commanders who unwittingly allow P2P to run unchecked on their networks are not exempt from liability. Commanders may be held personally liable for any illegal possession, storage, copying, or distribution of copyrighted materials that occurs on their networks. Soldiers, civilian employees and contractors face even tougher penalties.

People using P2P on government computers can look forward to other possibly harsher punishments depending on the kinds of files the users are sharing.

“Say you have a Soldier downloading music through P2P, in violation of copyright rules,” said Tom King, a legal adviser with NETCOM. “The people who own the copyright can actually sue that Soldier. Then you have the issue that he’s violating a lawful order. Then you have the issue that it’s a misuse of government time and misuse of a government resource. He can be in a world of hurt. Then he’s also exposing the Army network to hacking attacks.”

“Prosecutions are on the rise. Discipline is on the rise. People are taking this stuff more and more seriously all the time,” King said. “People just don’t understand that there’s a price to be paid for this.”

Not understanding seems to be the main reason P2P applications keep showing up on Army computer systems.

“User education is one of the keys,” said Kathy Buonocore, chief of the Regional Computer Emergency Response Team. “Some users don’t know it’s illegal.”

“When I call some commanders and tell them, they say, ‘What’s P2P?’” Andujar said. “Commanders have to be educated and take action.”

Education has to extend down to the organization administrators. Justiniano says those who have administrator privileges on government computer systems are the ones loading the unauthorized programs. To prevent this, system and network administrators should configure systems correctly, so users cannot install unauthorized software.

“There are very few benefits that are not addressed somewhere else, that do not include the risk of P2P software,” Justiniano said, adding that the use of Army Knowledge Online knowledge centers and secure File Transfer Protocol sites are their preferred method of file sharing.

(Editor’s note: Sgt. 1st Class Eric Hortin is a journalist for the U.S. Army Network Enterprise Technology Command.)

[Please click here to return to the previous page.](#)

Executive Order

EXECUTIVE DEPARTMENT

STATE OF CALIFORNIA



EXECUTIVE ORDER S-16-04
by the
Governor of the State of California

WHEREAS, the presence of certain peer-to-peer file-sharing software on state computers presents a significant security risk by potentially allowing individuals outside of the state system to access confidential and sensitive information that may be stored or maintained on state computers and networks; and

WHEREAS, use of some peer-to-peer file-sharing services on state government computers and networks can threaten the security and privacy of the information on those computers; and

WHEREAS, some peer-to-peer file-sharing services may permit viruses and other malicious programs to gain access to state computer systems; and

WHEREAS, use of some peer-to-peer file-sharing services consumes network resources, which may reduce the performance of state computer systems and impact the state's ability to effectively function and provide efficient services to the public; and

WHEREAS, while peer-to-peer technology holds the potential for many legitimate uses, currently peer-to-peer file-sharing services are often used to enable illegal dissemination and downloading of copyrighted material, including music, motion pictures, software and video games, resulting in huge losses of revenue to the state's valuable entertainment industry; and

WHEREAS, state government should take steps to ensure that state computers are not being used to disseminate or download copyrighted material through peer-to-peer file-sharing programs.

NOW, THEREFORE, I, ARNOLD SCHWARZENEGGER, Governor of the State of California, by virtue of the power and authority vested in me by the Constitution and statutes of the State of California, do hereby issue this order to become effective immediately:

1. For purposes of this Executive Order, "peer-to-peer file-sharing program" means computer software, other than computer and network operating systems, that has as its primary function the capability to allow the computer on which the software is used to designate files available for transmission to another computer using the software, to transmit files directly to another computer using the software, and to request the transmission of files from another computer using the software.
2. The State Chief Information Officer shall develop a statewide policy for use by each state agency, department, board, commission and office of the executive branch regarding the use of peer-to-peer file-sharing programs on state computers, including a prohibition of such programs that pose risks to the security and integrity of state computer systems. The policy shall not prohibit legitimate file-sharing between, among or within federal, state or local government entities for official business through the use of file-sharing programs that do not pose risks to the security and integrity of state computer systems or that are not used for illicit purposes. The head of each executive agency shall be responsible for ensuring compliance with the statewide policy.
3. The State Chief Information Officer shall explore the availability and cost effectiveness of filtering, screening or blocking

types of technology applicable for use on state government computers and networks.

4. The statewide policy provided for in this Executive Order shall not apply to the legislative and judicial branches of government, nor shall it apply to the constitutional officers of this state. However, I invite these branches of government and the constitutional officers to adopt and implement the statewide policy.

5. For the purposes of this order, the University of California and the California State University System are requested to comply with the statewide policy provided for in this Executive Order.



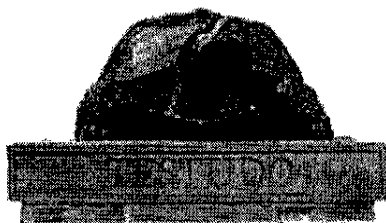
IN WITNESS WHEREOF I have here unto set my hand and caused the Great Seal of the State of California to be affixed this the sixteenth day of September 2004.

/s/ Arnold Schwarzenegger

Governor of California

[Back to Top of Page](#)

[Please click here to return to the previous page.](#)



THE DIAMONDBACK

THE UNIVERSITY OF MARYLAND'S INDEPENDENT STUDENT NEWS

NEWS _ SPORTS OPINION DIVERSIONS

Homepage About Advertising Archives/Search Contact Classifieds

www.diamondback

Jan 30, 2004

Governor pushed for file sharing warning

By Adam Lewis
Staff writer

A memorandum released to students, faculty and staff Wednesday night about the dangers of peer-to-peer file sharing was influenced by concerns from Gov. Bob Ehrlich's office about illegal downloading on state-owned networks, university officials said.

The letter, written by Provost Bill Destler and Mark Henderson, Office of Information Technology interim vice president and chief information officer, warned the university community about the possibility of criminal prosecution and the consequences of downloading copyrighted music and movies.

"Although downloading and trading copyrighted music, movies, games and software over the Internet has become commonplace with the advent of file-sharing programs such as KaZaa and Morpheus, those activities are frequently illegal," the letter said. "Members of the university community should refrain from illegal uses of P2P technology, thereby avoiding the ever-increasing risk of personal legal liability and disciplinary action and supporting the academic mission of the university."

Representatives from Ehrlich's office met with university officials over the past two months to discuss the problems of file sharing on the campus.

"We had some concerns expressed from the governor's office that the campus was one of the nationwide leaders in the downloading of music and movies from the P2P network," Destler said.

"A governor's office staff member met with university representatives last month to voice concerns about copyright-infringing file sharing on state-owned networks and to discuss educational and technological strategies we have in place or might consider," said OIT spokeswoman Amy Ginther. "We agreed that the memo was a strategy we would implement. We also intend to develop additional educational materials."

Representatives from Ehrlich's office could not be reached for comment.

The letter, which was sent out only via e-mail, noted the penalties students could face and the likelihood of being caught if they choose to illegally share copyrighted files.

The university is not the first to issue such a letter to its students.

"Many higher education institutions, including several of our peers, have distributed similar letters to their respective university communities," Ginther said. "We thought it was a good practice to highlight the issues in a visible manner in a letter to the entire community."

Today's Top Stories

Flood rips through Commons

5
Water shuts off in buildings around South Campus
By Laurie Au
Staff writer

University View opens with steep rental rates

Despite cost, student renters interested in luxury apartments
By Jason Flanagan and Laurie Au
Senior staff writers

Terps trying to buck losing streak, history

No. 5-ranked Florida St. holds 14-0 series lead
By Ryan Young
Senior staff writer

Officials within the recording industry were also concerned about file sharing on the campus, Destler said.

"I can tell you that we've gotten a number of very specific complaints from the recording industry about downloading from specific IP addresses on our network," he said.

OIT's Project NEThics is responsible for investigating incidents of misuse of computing resources and handling notices of copyright infringement. Although the letter's serious tone indicates increased concern over the potential for file sharing, Destler said it is not the university's role to ban P2P technology.

"I don't think we want to be enforcers of file-sharing policies," Destler said. "We want to place people in a position where they know what the issues are. Identifying and prosecuting offenders isn't our job."

Despite the prevalence of P2P file sharing among students, university officials said there are no current plans to create a legal music downloading alternative, as Penn State University did several months ago when they signed a contract with Napster 2.0 to provide music for its students.

"We are paying attention to the Penn State initiative and invite student input on whether they think such an option is viable," Ginther said.

At the same time, there are doubts about the feasibility of such a program.

"I've heard about Penn State's program and have some questions about it," Destler said. "There are circumstances where I would be interested in that, but from what I've heard, the Penn State contract doesn't seem like a good deal for our students."

Some students, however, have been supportive of the university's efforts to curb file sharing.

"Several e-mails from students were received, being very supportive. They were glad to hear the university was not shutting down file sharing," Destler said. "They were emphasizing the legitimate uses of P2P for other technology."

Even students who use file sharing technology say they agree with the university's policies.

"I don't download music because it's wrong, although I might be in the minority on that," said Brian Leigh, a junior electrical engineering major who uses Direct Connect to download episodes of television shows. "The policy could be stricter. It's so commonplace that anyone could do it."

Users of P2P technology, though, point out how difficult it is to enforce policies that discourage file sharing.

"I think it's a good policy, but I don't think it's very powerful," said William Lee, a freshman mathematics major who uses KaZaa to download movies. "Unless you can check every person's files, it's not going to stop."

try about downloading from specific IP addresses on our network," he said.

OIT's Project NEThics is responsible for investigating incidents of misuse of computing resources and handling notices of copyright infringement. Although the letter's serious tone indicates increased concern over the potential for file sharing, Destler said it is not the university's role to ban P2P technology.

"I don't think we want to be enforcers of file-sharing policies," Destler said. "We want to place people in a position where they know what the issues are. Identifying and prosecuting offenders isn't our job."

Despite the prevalence of P2P file sharing among students, university officials said there are no current plans to create a legal music downloading alternative, as Penn State University did several months ago when they signed a contract with Napster 2.0 to provide music for its students.

Some students have been supportive of the university's efforts to curb file sharing.

"Several e-mails from students were received, being very supportive. They were glad to hear the university was not shutting down file sharing," Destler said. "They were emphasizing the legitimate uses of P2P for other technology."

Even students who use file sharing technology say they agree with the university's policies.

"I don't download music because it's wrong, although I might be in the minority on that," said Brian Leigh, a junior electrical engineering major who uses Direct Connect to download episodes of television shows. "The policy could be stricter."

Users of P2P technology, though, point out how difficult it is to enforce policies that discourage file sharing.



DiamondbackOnline.com

Homepage | News | Sports | Opinion | Diversions | Web specials

About us | Contact us | Archives | Ad info | Classifieds

Traffic to Block Outbound to the Internet

Currently the State of Michigan allows unfiltered access to the Internet for its employees. The industry best practice is to universally deny access to the Internet and then only allow specific traffic when an appropriate business reason is established.

Moving directly to the industry standard all at once would have a negative impact on existing State business. As a first step outbound Internet access for the applications/services below will be restricted. The applications/services of the first phase are not known to support the State's business, invite unacceptable use by employees, and greatly increase risk to the State's network.

PHASE ONE (Beginning 3/25/04) -

Peer-to-Peer File Sharing:

- Kazaa
- Gnutella Network (e.g. Gnutella, Limewire, Bearshare, Morpheus, etc...)
- eDonkey and eMule
- DirectConnect Network
- Overnet
- WinMX
- MP2P Network (RockitNet, Blubster, Pilolet)
- Napster

Known Trojans/Backdoors:

- Back Orifice (2000)
- SubSeven
- Netbus

Games:

- MSN Gaming Zone
- Yahoo Games
- Xbox Game port
- Multi-User Dungeons (MUD)

Remote Control Programs:

- PC Anywhere
- Timbuktu
- GoToMyPc
- Terminal Services
- VNC

Other:

- AOL VPN
- Spyware/Adware
- SNMP
- tFTP
- Services/Ports not used in the last six weeks

PHASE TWO (TBD) -

Instant Messaging:

IRC
AIM, ICQ
YahooIM
MSN
Trillian

Internet Mail:

SMTP
POP-3

United States Senate

WASHINGTON, DC 20510

May 4, 2004

The Honorable Timothy J. Muris, Chairman
The Honorable Mozelle W. Thompson, Commissioner
The Honorable Orson Swindle, Commissioner
The Honorable Thomas B. Leary, Commissioner
The Honorable Pamela Jones Harbour, Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Dear Mr. Chairman and Commissioners:

We write to request that the Federal Trade Commission (the "Commission") determine whether various provisions of the Federal Trade Commission Act (the "Act") are being violated by the designers, publishers, distributors and operators of certain iterations of software commonly known as "peer-to-peer file-sharing software." These parties have distributed this software widely and for free - frequently to unsupervised children. In fact, nearly half of the users of this software may be children. This software not only enables children and others to make "free" infringing copies of copyrighted music, movies, software and games for their own use, but also may unwittingly turn each user into an illegal re-distribution center for both copyrighted works and child pornography.

Recently, a federal court found that certain publishers and distributors of filesharing software "may have intentionally structured their businesses to avoid secondary liability for copyright infringement, while benefiting financially from the illicit draw of their wares." If this is true, then those distributing P2P software to consumers and children may be failing to disclose profound risks associated with foreseen, widespread uses of their products. If so, then the Commission should consider the appropriate steps it may take to protect our citizens and children from potentially unfair and deceptive trade practices that mislead and endanger.

This software inarguably poses dangers even when it is used as intended in ways that were foreseeable and have become common practice. Many children use this software to download popular songs: They risk significant civil penalties for copyright infringement and criminal convictions for re-distributing infringing works to pirates around the world. Many adults use this software to download adult pornography for their own private viewing: They may risk criminal convictions for distributing this pornography to minors. Something is horribly wrong when millions use a product in ways that are illegal, dangerous to them, and dangerous to others.

We stress that risks like these are *not* inherent in the use of computers, the Internet, or even most software that can transfer files between "peer" computers. Instead, they appear to arise when particular file-sharing software is distributed with default settings and other attributes that seem designed to facilitate widespread, ongoing copyright piracy and trafficking in pornography. Two features of such designs seem to generate these unusual risks.

First, such software enables what might be called "dark-alley file-sharing": Through a combination of unenforced use "limitations" and licenses, pseudo-anonymity, and automatic program features that operate without the user's intervention or knowledge, this type of software creates shadowy "dark alleys" in cyberspace. In those dark alleys, you can get things - though you aren't sure what they really are - from strangers who cannot be later identified or held accountable. Unsurprisingly, these dark alleys tend to become havens for piracy, pornography and computer viruses.

Second, such software enables so-called "viral" redistribution: By default, users of the software make all files downloaded available for redistribution to other users. This "viral" redistribution can thwart enforcement of the rights of artists because one infringing copy of a popular work can quickly multiply over a network. "Viral" redistribution works by turning mere *consumers* of content into international *distributors* of content. As a result, people seeking content to use at home can inadvertently incur all the complex and unfamiliar risks of managing an international content-distribution operation.

We cannot detail all of the risks to consumers that arise when dark-alley file-sharing combines with "viral" redistribution. We summarize only some of these risks, which may be grouped into three broad categories: pornography, piracy and data security.

Pornography and Child Pornography: Recent research suggests that pornography downloading has joined music piracy as a leading use of much dark-alley file-sharing software. Much of this pornography is disturbing and potentially obscene: It may depict hardcore sex, sadism, masochism, violence, bestiality, or rape. The prevalence and nature of this pornography endangers users of this software in at least three ways.

First, filesharing is based on searchable lists, which may contain deceiving file names, with the result that the program delivers graphic pornography even to children searching for innocent content. Unenforced end-user licenses frequently let the worst pornography link itself to innocent subjects. For example, the Government Accounting Office (GAO) reported to Congress that "searches on innocuous keywords likely to be used by juveniles" retrieved images including adult pornography (34 %), cartoon pornography (14%), child pornography (1%) and child erotica (7%). Searching some networks for terms like "Olsen twins" and "Harry Potter" will return files whose very names describe sex crimes. "Pokemon" cartoons, music, and movies are designed to attract young children - yet one search for "Pokemon" returned files purporting to depict the rape of Pokemon's child-stars.

Some file-sharing software promotes "keyword" filters as a means to protect file-sharing children from pornography. But "keyword" filters can only prevent children from searching for pornography - not from exposure to the pornography responsive even to innocuous searches. For example, when one such "Family Filter" was engaged, a search for the term "horse" returned images of graphic bestiality. Such filters can also be easily disabled, even by children. In any event, unaccountable pornographers can circumvent these filters by mislabeling pornographic files with misleading filenames and metadata.

Second, file-sharing can expose unwitting children or adults to profoundly disturbing child pornography that is illegal to possess, view, or distribute. Pedophiles use filesharing to distribute illegal child pornography. Searches of popular filesharing networks have returned files with names like "13-year-old lolita raped and crying." Suffolk County District Attorney Thomas Spota told the Senate Committee on the Judiciary that one popular network distributed the videotaped rape of a toddler in diapers. GAO has confirmed that some of this illegal child pornography is mislabeled so it will appear in response to innocuous searches.

Third, "viral" redistribution of *any* pornography can endanger not only children, but also *adults who want to view adult pornography*. For example, imagine a college student, who uses file-sharing software as intended to download for private use a violent adult pornographic image. Automatically, however, the P2P program itself makes the image accessible for downloading by every other user of the file-sharing software, including children or users who live in different areas of the country with different community standards. As a result, this student may redistribute violent pornography to children and others - and risk criminal prosecution under state or federal criminal laws governing pornography distribution. Both Congress and the Department of Justice have advised prosecutors to target obscenity prosecutions toward pornography *distributors* - particularly those who distribute to minors.

Unfortunately, this is no hypothetical. It is happening now. Otherwise law-abiding adults who may only have meant to view pornography privately are - intentionally, negligently or unknowingly - becoming pornography distributors who distribute world-wide, to children and adults. We doubt that most such adults realize how "viral" redistribution of *any* pornography endangers both adults and children.

Copyright Infringement: File-sharing can also expose children and consumers to severe civil and criminal penalties for copyright infringement. The enduring prevalence of this piracy strongly suggests that some who profit from it have failed to educate their users about the many dangers of infringing copyrights.

Testimony and news reports show that some users of file-sharing software - particularly children - do not yet realize that downloading popular music or movies "for free" is usually unlawful. Many users may not realize that downloading or redistributing infringing works can be a federal crime, and may not know the severity of the penalties for copyright infringement. These users cannot be adequately educated by vague warnings to "obey the law": Review of the Copyright Act will not disclose which files

may be illegal to download, the prevalence of infringing works on a network, or the risks of letting a clever designer limit his own risks of liability by using your home computer to house network search indices much like those that exposed the original Napster to staggering secondary liability for infringement.

Data Security: Most dark-alley file-sharing software can redistribute any kind of file, including audio, images, documents and video. Such software can thus compromise the security of any data stored on the hard drive of a personal computer. People now use their computers to store highly sensitive data, including personal finances, tax returns, photographs, correspondence, business documents, and emails. Much of this data - if broadcast to millions of other Internet users - could facilitate identity theft.

Research by computer scientists Nathaniel Good and Aaron Kreckelberg has revealed that (1) thousands of people seem to have inadvertently shared profoundly personal data over filesharing networks, and (2) malicious users are accessing files that seem to contain sensitive data like credit card numbers. Other research conducted by the Committee on Government Affairs of the House of Representatives reveals that thousands are sharing data files that probably contain detailed records of their personal finances, including account numbers, credit card numbers, and individual financial transactions. Indeed, last year, PC Magazine reported that downloading the inadvertently shared personal data of others had become the latest filesharing "fad."

In addition to inadvertently sharing sensitive personal, business, or government data, users may also compromise their security and risk identity theft by downloading files that conceal malicious viruses, Trojan-horse programs or backdoors. New research by the security company TruSecure has revealed that about 60% of the nearly 5000 executable files downloaded with popular filesharing software contained such viruses, Trojan-Horse programs or backdoors. Some were concealed in games popular among children. PC Magazine also recently reported that one of the most recent widespread infections, the "MyDoom [virus] seems to have started on KaZaA, the popular peer-to-peer filesharing service." PC Magazine also reported potential problems with the antivirus program in Kazaa that may have rendered it largely useless during the MyDoom outbreak.

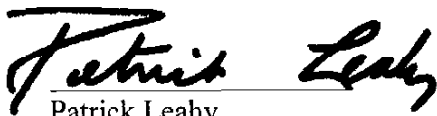
Finally, too much dark-alley file-sharing software helps its creators profit from piracy and pornography by installing so-called "adware" or "spyware" programs. These programs can compromise the privacy of every person who uses a given computer - *even if they never use filesharing software or consent to its installation*. We commend the Commission for opening an investigation of this issue.

In sum, the dangers of file-sharing software are real, and consumers need to be protected. The Act directs the Commission to protect consumers from "unfair or deceptive acts or practices" that affect commerce. 15 U.S.C.A. § 45(a)(1). If the designers, publishers, and distributors of file-sharing software have not adequately warned users about the risks of using their software, and are intentionally distributing the software in a manner that increases risks to end-users, then they have endangered their customers - and our children. These entities - many of whom profit primarily through advertising or sales of

“premium” versions - from illicit uses of their software - must effectively educate even their youngest users about the dangers of their software.

We request that the Commission investigate these issues during its upcoming hearings. We further request that the Commission report back on (1) the results of its investigation, (2) how it intends to redress any problems disclosed under existing law, and (3) whether existing law provides adequate authority to redress any and all problems disclosed. We also request that the Commission commence and prosecute any enforcement actions justified by any potential violations of the Act disclosed.

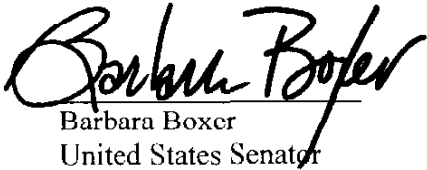
Sincerely,



Patrick Leahy
United States Senator



Orrin G. Hatch
United States Senator



Barbara Boxer
United States Senator



Ted Stevens
United States Senator



Gordon Smith
United States Senator

01/23/04 FRI 13:59 FAX 202 223 3003

001

United States Senate

WASHINGTON, DC 20510

November 12, 2003

Daniel Rung, Owner, Grokster
Vincent Falco, President, BearShare
Wayne Rosso, President, Blubster
Sam Yagan, President, oDonkey 2000
Greg Bildson, President, Lime Wire
Michael Weiss, President, Streamcast Networks
c/o P2P United
1317 F Street, NW, Suite 800
Washington, DC 20004

Nikki Hemming, CEO, Sharman Networks
c/o Distributed Computing Industry Association
4200 Wilson Blvd, Suite 800
Arlington, VA 22203

Dear Messrs. Rung, Falco, Rosso, Yagan, Bildson, and Weiss, and Ms. Hemming,

Following several recent Congressional hearings focusing on the copyright infringement and pornography problems associated with the use of peer-to-peer technology, we are writing to ask some important questions about your business practices.

Although we believe that P2P technology has tremendous positive potential, to date, that potential is far from realized. Recent studies by the General Accounting Office and Palisades Systems, a respected technology company, clearly demonstrate that your software currently is being used almost exclusively as a means of illegally trading copyrighted material and distributing pornography, including child pornography. For example, the Palisades report concluded that 97% of all the material available on file-sharing services was either copyrighted or pornography; 99% of audio files requested on file-sharing services were copyrighted; and 42% of all requests on file-sharing services were for adult or child pornography. Fulfilling the professed promise of P2P will never occur as long as it remains a platform predominately used for copyright infringement and illegal access to pornography.

We are writing to encourage you to voluntarily take the following three common-sense steps to reverse this troubling trend and help educate and protect P2P users.

1. **Provide a Clear, Conspicuous, and Meaningful Notice & Warning to Users about the Legal Risks of Using P2P Software**

In the wake of the recent lawsuits by the Recording Industry Association of America, a New York Times article, "Is It Wrong to Share your Music", September 18, 2003, noted that: "Sony, Korbi and others in the class [7th & 8th] graders complained about the mixed signals they get from those who are supposedly responsible for

informing them what is right and wrong. That includes . . . the purveyors of such programs as Kazaa, which allow the downloading to take place -- "Why isn't there a warning that what we're doing is illegal?" Unfortunately, these 7th and 8th graders are not alone -- millions of parents and children around the nation are now asking the same question.

Will your company take responsibility for educating consumers by immediately beginning to provide a clear, conspicuous and meaningful warning to users, before they download your software, that using the software to "share" copyrighted music is clearly illegal under existing law, and that doing so may subject them to lawsuits like the ones recent filed by the RIAA?

2. **Incorporate Effective Copyright and Pornography Filters**

Two well-respected technologists recently pointed out that your company could easily take steps to reconfigure your software to significantly reduce or prevent copyright infringement and pornography. According to Professor Leonard Kleinrock of the UCLA Computer Science Department: "There is nothing inherent in the technology . . . of peer-to-peer system[s] that would prevent [them] from taking steps to prevent or greatly diminish the volume of copyright infringement on their systems." And Darrell Smith, the former CTO of the file-sharing service Morpheus (StreamCast Networks) noted that: "Peer-to-peer file sharing applications already filter those things that their users do not want, such as bogus music files and viruses. They could very easily adopt and implement a filter to eliminate unauthorized copyrighted works as well, but user levels and revenues could decline if popular music or movie files were filtered."

Will your company incorporate effective copyright and pornography filters into your software in an effort to reduce or prevent copyright infringement and illegal access to pornography?

3. **Change the "Sharing" Default Setting**

It is a clear violation of U.S. Copyright laws to distribute a copyrighted work without the owner's permission. Yet, by default, P2P software is designed so that every copyrighted file users download they automatically distribute to everyone else on the network. So the only way to avoid being a forced distributor, and thereby avoid being subject to a copyright infringement lawsuit for "sharing", is to change the default settings that come with the software.

Will your company help users avoid copyright liability by changing the automatic "sharing" setting in their P2P software so that users are required affirmatively to choose to share files instead of being required to as a default?

We strongly believe that voluntarily taking these three common-sense steps would go a long way toward educating and protecting consumers. It also would clearly indicate your

company's desire to become responsible corporate citizens. We look forward to written answers to each of our questions by December 15, 2003.

Sincerely,

LINDSEY O. GRAHAM
United States Senator

DIANNE FEINSTEIN
United States Senator

RICHARD J. DURBIN
United States Senator

GORDON SMITH
United States Senator

JOHN CORNYN
United States Senator

BARBARA BOXER
United States Senator

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL
750 FIRST STREET NE SUITE 1100
WASHINGTON, D.C. 20002
(202) 326-6016
(202) 349-1921
<http://www.naag.org>

LYNNE M. ROSS
Executive Director

August 5, 2004

PRESIDENT
WILLIAM H. SORRELL
Attorney General of Vermont

PRESIDENT-ELECT
STEPHEN CARTER
Attorney General of Indiana

VICE PRESIDENT
THURBERT BAKER
Attorney General of Georgia

IMMEDIATE PAST PRESIDENT
BILL LOCKYER
Attorney General of California

Adam Eisgrau, Executive Director
P2P United
c/o Flanagan Consulting LLC
1317 F Street, N.W., Suite 800
Washington, D.C. 20004

Re: Peer-to-Peer Software

Dear Mr. Eisgrau:

We are writing to encourage your companies to take concrete and meaningful steps to address the serious risks posed to the consumers of our States by your company's peer-to-peer ("P2P") file-sharing technology. By addressing such problems today as the use of P2P networks to disseminate pornography, invade privacy and infringe copyrights, P2P software may one day realize its potential as a means for facilitating a wide range of collaborative, project management, business planning, and academic/education activities. At present, P2P software has too many times been hijacked by those who use it for illegal purposes to which the vast majority of our consumers do not wish to be exposed.

We have carefully considered your response to the issues raised by P2P software as presented during the June 15-18, 2004 Summer Meeting of the National Association of Attorneys General and the June 8-9, 2004 National Association of Attorneys General Internet Conference. However, we find that this response fails to address the issues raised by P2P software.

Our consumers need to be provided with the information necessary to understand this technology and to make informed decisions concerning its use. P2P file-sharing technology works by allowing consumers to download free software that enables them to directly share files stored on their hard drive with other users. This type of direct access to one's computer differentiates P2P file-sharing technology from garden-variety e-mail accounts and commercial search engines such as Google and Yahoo.

One substantial and ever-growing use of P2P software is as a method of disseminating pornography, including child pornography. While at least some of your companies do provide “filters” to help screen out unwanted files, including presumably those containing pornography, those filters appear to work by focusing on language in the file’s description or the file’s title rather than on the file’s content. P2P users interested in disseminating and receiving offensive or illegal material, such as child pornography, can simply use an innocuous file title and/or description in order to bypass those filters. Consequently, P2P users need to be made aware that they are exposing themselves, and their children, to widespread availability of pornographic material when they download and install P2P file-sharing programs on their computers.

Furthermore, P2P file-sharing technology can allow its users to access the files of other users, even when the computer is “off” if the computer itself is connected to the Internet via broadband. P2P users, including both home users and small businesses, who do not properly understand this software have inadvertently given other P2P users access to tax returns, medical files, financial records, personal e-mail, and confidential documents stored on their computers. Combating identity theft is one of our priorities, and many of our States have enacted laws to stop it. Consequently, P2P users need to be properly educated so that they will not inadvertently share personal files on their hard drives with other users of your P2P file-sharing technology.¹

The illegal uses of P2P technology are having an adverse impact on our States’ consumers, economies, and general welfare. There are serious concerns that P2P software is replacing Internet chat rooms and e-mail as a medium of choice for the dissemination of pornography, especially child pornography. Market forces and technological limitations of the Internet (e.g., the need to pay for web space and bandwidth) have combined to make peer-to-peer software a more attractive alternative to the Internet as a means of disseminating pornography. Peer-to-peer users and distributors of child pornography particularly believe that their anonymity on P2P networks protects them from detection by law enforcement. According to a January 25, 2004 New York Times Magazine article, “[c]yber networks like KaZaa and Morpheus – have become the Mexican border of virtual sexual exploitation.” The Federal Trade Commission, the United States General Accounting Office, and the Judiciary Committee of the United States Senate, among others, have all taken testimony or issued reports on the increasing use of P2P software to disseminate pornography.

P2P file-sharing programs also are being used to illegally trade copyrighted music, movies, software, and video games, contributing to economic losses. The Business Software Alliance estimates that its members lost \$13 billion in revenue last year due to software piracy. According to a February 20, 2004 CNN article, “U.S. software companies lose up to \$12 billion a year in piracy according to the Software and Information Industry Association. Music companies lost more than \$4.6 billion worldwide last year, according to the RIAA [Recording Industry Association of America] and movie industry officials pegged their annual losses from bootlegged films at more than \$3.5 billion.”

¹ This problem is exacerbated by the default settings that you use as part of the installation process of P2P software. One default setting designates each and every file in a user’s hard drive for sharing with other users of P2P software. A second default setting leaves a user’s computer continuously accessible to the Internet. We would urge your companies not to select such default settings as part of your software installation process.

The article further reveals that “[t]he entertainment and computer industry have tried to stem piracy by making CDs and DVDs harder to duplicate. But the rise of free file-sharing networks on the Internet has made it easy for millions of individuals to distribute songs, movies, and software worldwide.” Similarly, a March 28, 2003 USA Today article described a recent hearing of the California Senate Select Committee on the Entertainment Industry in which “committee chairman Kevin Murray, D-Los Angeles, downloaded the KaZaa media desktop player in under 20 seconds, then downloaded numerous songs and the Oscar-winning movie *Chicago*, which hasn’t been released on DVD.”

Some of your companies have taken initial steps to warn users of P2P software that it may not be employed for illegal ends, which is commendable. However, more needs to be done by your companies to warn your P2P users as to the specific legal and personal risks they face when they use P2P technology for the illegal ends of disseminating pornography and “sharing” copyrighted music, movies, and software.

We have, in the past, initiated Internet-related actions to stop individuals from disseminating unwanted spam, including deceptive e-mail designed to lure unsuspecting adults and children to pornographic web sites. We will, as appropriate, continue to initiate such actions in the future to stop deceptive and illegal practices by users of the Internet, including users of P2P software.

However, the undertaking of enforcement actions against individual users does not excuse your companies from fostering deceptive practices on our consumers that invade their privacy and threaten their security. Nor do they excuse your companies from avoiding software design changes that deliberately prevent law enforcement in our States from prosecuting P2P users for violations of the law.

We view with alarm reports that P2P software is being used by your companies as a means of transmitting unwanted spyware and adware that is bundled with the P2P software. Spyware aids an individual or a corporation in gathering information about P2P users without their consent or in asserting control over P2P users’ computers without their consent. In the past, we have initiated enforcement actions against Internet web sites that, without the knowledge of our consumers, placed “cookies” on their computers designed to track their use of the Internet. We would ask you to take concrete and meaningful steps to avoid the infringement of the privacy and security of our citizens by bundling unwanted spyware and adware with your software.²

We view with equal alarm reports that at least some P2P file-sharing services are adding encryption features to those services. The addition of such encryption features will make it more difficult, if not impossible, for law enforcement to police users of P2P technology in order to prosecute crimes such as child pornography. Encryption only reinforces the perception that P2P technology is being used primarily for illegal ends. Accordingly, we would ask you to refrain from making design changes to your software that prevent law enforcement in our States from investigating and enforcing the law.

² It also has come to our attention that P2P file-sharing technology is being used as a means of transmitting computer viruses and worms because conventional virus protection programs, such as those marketed by Novell, do not scan files exchanged via such technology. If such is the case, then it would be incumbent upon your companies to warn your users of this risk.

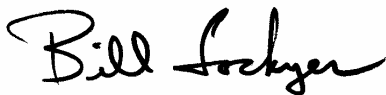
Finally, we are concerned that the filters currently in use are inadequate as a means of protecting P2P users, and their children, from unwanted and offensive materials, such as child pornography. We believe that meaningful steps can and should be taken by the industry to develop more adequate filters capable of better protecting P2P parents and children from unwanted or offensive material. Not warning parents about the presence of, and then reasonably providing them with the ability to block or remove, obscene and illegal materials from their computers is a serious threat to the health and safety of children and families in our States.

We take seriously our responsibility to protect our citizens from misleading or deceptive practices, and to ensure that our citizens are given the information necessary to making an informed decision. And, we take seriously the need to investigate and prosecute violations of our laws wherever they may be taking place – on the Internet, in the brick and mortar world, or on P2P networks.

We believe that it is in no one's interest for P2P technology to be used in order to promote unlawful or deceptive activities. Rather, we believe that concrete and meaningful steps can and should be taken to address the problems we have raised in this letter. It is only by taking such steps that P2P networks will be able to realize their innovative potential as a 21st century virtual collaboration and project management tool for regional or nationwide academic, business, home, and governmental activities.

We look forward to working closely with you to proactively address these problems.

Sincerely,



BILL LOCKYER
Attorney General of California



GREG ABBOTT
Attorney General of Texas



CHARLIE CRIST
Attorney General of Florida



TROY KING
Attorney General of Alabama



TERRY GODDARD
Attorney General of Arizona



MIKE BEEBE
Attorney General of Arkansas



KEN SALAZAR
Attorney General of Colorado



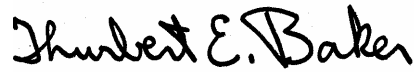
RICHARD BLUMENTHAL
Attorney General of Connecticut



M. JANE BRADY
Attorney General of Delaware



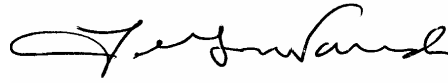
ROBERT J. SPAGNOLETTI
Attorney General of the District of Columbia



THURBERT BAKER
Attorney General of Georgia



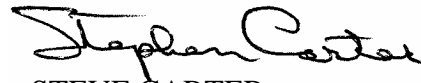
MARK J. BENNETT
Attorney General of Hawaii



LAWRENCE WASDEN
Attorney General of IDADHO



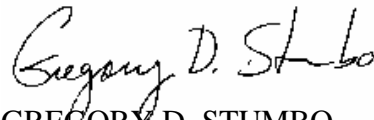
LISA MADIGAN
Attorney General of Illinois



STEVE CARTER
Attorney General of Indiana



TOM MILLER
Attorney General of Iowa



GREGORY D. STUMBO.
Attorney General of Kentucky



CHARLES C. FOTI JR.
Attorney General of Louisiana



STEVE ROWE
Attorney General of Maine



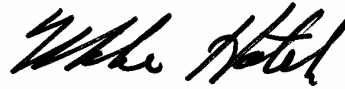
J. JOSEPH CURRAN JR.
Attorney General of Maryland



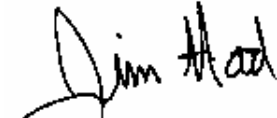
THOMAS F. REILLY
Attorney General of Massachusetts



MICHAEL COX
Attorney General of Michigan




MIKE HATCH
Attorney General of Minnesota



JIM HOOD
Attorney General of Mississippi



JEREMIAH W. NIXON
Attorney General of Missouri



MIKE MCGRATH
Attorney General of Montana



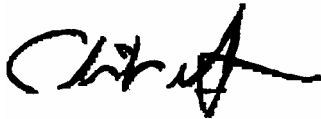
BRIAN SANDOVAL
Attorney General of Nevada



PETER C. HARVEY
Attorney General of New Jersey



PATRICIA MADRID
Attorney General of New Mexico



ELIOT SPITZER
Attorney General of New York



ROY COOPER
Attorney General of North Carolina



WAYNE STENEHJEM
Attorney General of North Dakota



JIM PETRO
Attorney General of Ohio



W.A. DREW EDMONDSON
Attorney General of Oklahoma



HARDY MYERS
Attorney General of Oregon



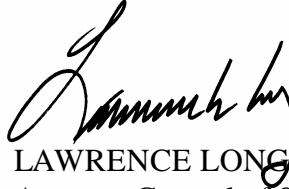
GERALD J. PAPPERT
Attorney General of Pennsylvania



PATRICK LYNCH
Attorney General of Rhode Island



HENRY MCMASTER
Attorney General of South Carolina



LAWRENCE LONG
Attorney General of South Dakota



PAUL SUMMERS
Attorney General of Tennessee



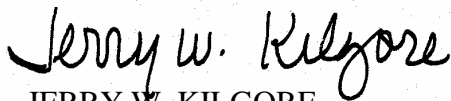
MARK SHURTLEFF
Attorney General of Utah



WILLIAM H. SORRELL
Attorney General of Vermont



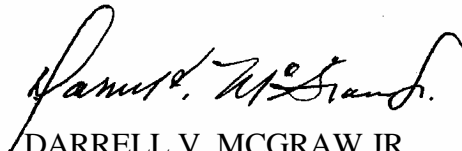
IVER STRIDIRON
Attorney General of the Virgin Islands



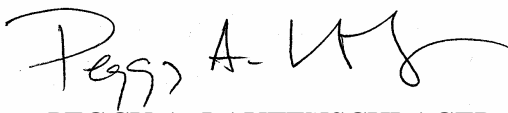
JERRY W. KILGORE
Attorney General of Virginia



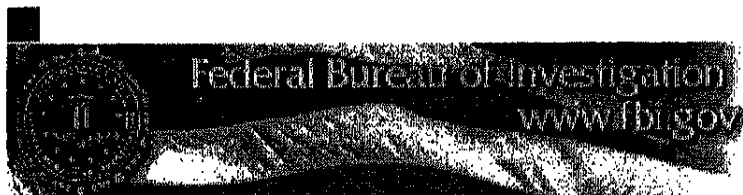
CHRISTINE O. GREGOIRE
Attorney General of Washington



DARRELL V. MCGRAW JR.
Attorney General of West Virginia



PEGGY A. LAUTENSCHLAGER
Attorney General of Wisconsin



[FBI Priorities](#)
[About Us](#)
[Press Room](#)
[Investigative Programs](#)
[Counterterrorism](#)
[Most Wanted](#)
[Field Divisions](#)
[Reports & Publications](#)
[FBI History](#)
[For the Family](#)
[Employment](#)
[Search](#)
[Home](#)

Investigative Programs Cyber Investigations

Cyber Education Letter

To Users of Peer-to-Peer Systems:

The FBI has undertaken a new initiative to educate and warn citizens about certain risks and dangers associated with the use of Peer-to-Peer systems on the Internet. While the FBI supports and encourages the development of new technologies, we also recognize that technology can be misused for illicit and, in some cases, criminal purposes. In an effort to help citizens learn how to protect themselves, this letter is being distributed and is posted on the FBI's web site at www.fbi.gov/cyberinvest/cyberedletter.htm.

[New! Cyber Education Letter](#)

[File a Complaint through the Internet Fraud Complaint Center](#)

[Internet Crime Complaint Center](#)

[Online Child Pornography Program](#)

[National Center for Missing and Exploited Children](#)

[New E-Scams & Warnings](#)

[Cyber Investigations Home](#)

[Submit A Tip](#)

[Apply Today](#)

[Links](#)

[Contact Us](#)

[Site Map](#)

[Privacy Policy](#)

Peer-to-Peer networks allow users connected to the Internet to link their computers with other computers around the world. These networks are established for the purpose of sharing files. Typically, users of Peer-to-Peer networks install free software on their computers which allows them (1) to find and download files located on another Peer-to-Peer user's hard drive, and (2) to share with those other users files located on their own computer. Unfortunately sometimes these information-sharing systems have been used to engage in illegal activity. Some of the most common crimes associated with Peer-to-Peer networks are the following:

Copyright Infringement: It is a violation of Federal law to distribute copyrighted music, movies, software, games, and other works without authorization. There are important national economic consequences associated with such theft. The FBI has asked industry associations and companies that are particularly concerned with intellectual property theft to report to the FBI -- for possible criminal investigation and prosecution -- anyone that they have reason to believe is violating Federal copyright law.

Child Exploitation and Obscenity: The receipt or distribution of child pornography and unlawful obscenity over the Internet also is a serious Federal crime. The FBI cautions parents and guardians that, because there is no age restriction for the use of Peer-to-Peer services, pornography of all types is easily accessible by the many young children whose parents mistakenly believe they are only accessing music or movies. In fact, children may be exposed to pornography -- and subsequently lured by sexual predators -- even though they were not searching for pornography, as some network users deliberately mislabel the names of files for this purpose.

Computer Hacking: Peer-to-Peer networks also have been abused by hackers. Because these systems potentially expose your computer and files to millions of other users on the network, they also expose your computer to worms and viruses. In fact, some worms have been specifically written to spread by popular Peer-to-Peer networks. Also, if Peer-to-Peer software is not properly configured, you may be unknowingly opening up the contents of your entire hard drive for others to see and download your private information.

The FBI urges you to learn about the risks and dangers of Peer-to-Peer networks, as well as the legal consequences of copyright infringement, illegal pornography, and computer hacking. For more information about the law, visit www.usdoj.gov/criminal. The FBI takes seriously its mission to enforce the laws against those who use the Internet to commit crime. To report cyber crime, please contact your local FBI Field Office, www.fbi.gov/contact/fo/fo.htm or file a complaint through the Internet Crime Complaint Center at www.IC3.gov.

FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer and Business Education

File-Sharing: A Fair Share? Maybe Not.

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- **Set up the file-sharing software very carefully.** If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.
- **Be aware of spyware.** Some file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, you may want to buy software that can prevent the downloading of spyware or help detect it on your hard drive.
- **Close your connection.** In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.
- **Use and update your anti-virus software regularly.** Files you download could be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Although your virus

filter should prevent your computer from receiving possibly destructive files, computer security experts suggest you avoid files with extensions like *.exe*, *.scr*, *.lnk*, *.bat*, *.vbs*, *.dll*, *.bin*, and *.cmd*.

- **Talk with your family about file-sharing.** Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files sometimes are mislabeled, kids unintentionally may download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.



GAO

Report to the Chairman and Ranking
Minority Member, Committee on
Government Reform, House of
Representatives

February 2003

FILE-SHARING PROGRAMS

Peer-to-Peer Networks Provide Ready Access to Child Pornography



Highlights of [GAO-03-351](#), a report to the Chairman and Ranking Minority Member, Committee on Government Reform, House of Representatives

Why GAO Did This Study

The availability of child pornography has dramatically increased in recent years as it has migrated from printed material to the World Wide Web, becoming accessible through Web sites, chat rooms, newsgroups, and now the increasingly popular peer-to-peer file-sharing programs. These programs enable direct communication between users, allowing users to access each other's files and share digital music, images, and video.

GAO was requested to determine the ease of access to child pornography on peer-to-peer networks; the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, including child pornography; and the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks.

Because child pornography cannot be accessed legally other than by law enforcement agencies, GAO worked with the Customs Cyber-Smuggling Center in performing searches: Customs downloaded and analyzed image files, and GAO performed analyses based on keywords and file names only.

In commenting on a draft of this report, the Department of Justice agreed with the report's findings and provided additional information.

www.gao.gov/cgi-bin/getrpt?GAO-03-351.

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

FILE-SHARING PROGRAMS

Peer-to-Peer Networks Provide Ready Access to Child Pornography

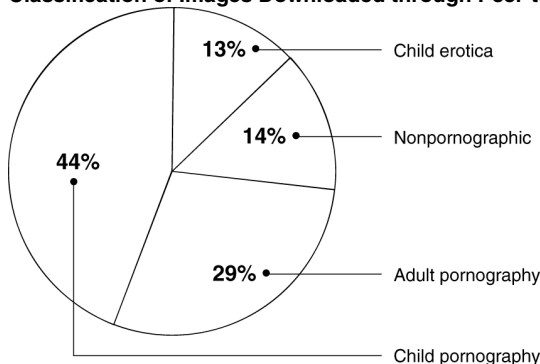
What GAO Found

Child pornography is easily found and downloaded from peer-to-peer networks. In one search using 12 keywords known to be associated with child pornography on the Internet, GAO identified 1,286 titles and file names, determining that 543 (about 42 percent) were associated with child pornography images. Of the remaining, 34 percent were classified as adult pornography and 24 percent as nonpornographic. In another search using three keywords, a Customs analyst downloaded 341 images, of which 149 (about 44 percent) contained child pornography (see the figure below). These results are in accord with increased reports of child pornography on peer-to-peer networks; since it began tracking these in 2001, the National Center for Missing and Exploited Children has seen a fourfold increase—from 156 in 2001 to 757 in 2002. Although the numbers are as yet small by comparison to those for other sources (26,759 reports of child pornography on Web sites in 2002), the increase is significant.

Juvenile users of peer-to-peer networks are at significant risk of inadvertent exposure to pornography, including child pornography. Searches on innocuous keywords likely to be used by juveniles (such as names of cartoon characters or celebrities) produced a high proportion of pornographic images: in our searches, the retrieved images included adult pornography (34 percent), cartoon pornography (14 percent), child erotica (7 percent), and child pornography (1 percent).

While federal law enforcement agencies—including the FBI, Justice's Child Exploitation and Obscenity Section, and Customs—are devoting resources to combating child exploitation and child pornography in general, these agencies do not track the resources dedicated to specific technologies used to access and download child pornography on the Internet. Therefore, GAO was unable to quantify the resources devoted to investigating cases on peer-to-peer networks. According to law enforcement officials, however, as tips concerning child pornography on peer-to-peer networks escalate, law enforcement resources are increasingly being focused on this area.

Classification of Images Downloaded through Peer-to-Peer File-Sharing Program



Source: Customs CyberSmuggling Center.

Contents

Letter		1
	Results in Brief	2
	Background	3
	Peer-to-Peer Applications Provide Easy Access to Child Pornography	11
	Juvenile Users of Peer-to-Peer Applications May Be Inadvertently Exposed to Pornography	14
	Federal Law Enforcement Agencies Are Beginning to Focus Resources on Child Pornography on Peer-to-Peer Networks	15
	Conclusions	17
	Agency Comments and Our Evaluation	17
Appendix I	Objectives, Scope, and Methodology	19
Appendix II	Description of File Sharing and Peer-to-Peer Networks	21
Appendix III	Comments from the Department of Justice	26
Glossary		29
Tables		
	Table 1: Internet Technologies Providing Access to Child Pornography	7
	Table 2: Organizations and Agencies Involved with Peer-to-Peer Child Pornography Efforts	9
	Table 3: NCMEC CyberTipline Referrals to Law Enforcement Agencies, Fiscal Years 1998–2002	14
Figures		
	Figure 1: Classification of 1,286 Titles and File Names of Images Identified in KaZaA Search	12
	Figure 2: Classification of 341 Images Downloaded through KaZaA	13

Figure 3: Classification of 177 Images of a Popular Singer, Child Actors, and a Cartoon Character Downloaded through KaZaA	15
Figure 4: Peer-to-Peer Models	22
Figure 5: Topology of a Gnutella Network	25

Abbreviations

CEOS	Child Exploitation and Obscenity Section
FBI	Federal Bureau of Investigation
IRC	Internet Relay Chat
MP3	Moving Pictures Experts Group (MPEG) MPEG-1 Audio Layer-3
NCMEC	National Center for Missing and Exploited Children
NCVIP	National Child Victim Identification Program
NRC	National Research Council
P2P	peer to peer
URL	Uniform Resource Locator
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. It may contain copyrighted graphics, images or other materials. Permission from the copyright holder may be necessary should you wish to reproduce copyrighted materials separately from GAO's product.



G A O

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

February 20, 2003

The Honorable Tom Davis
Chairman
The Honorable Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
House of Representatives

The availability of child pornography has dramatically increased in recent years as it has migrated from magazines, photographs, and videos to the World Wide Web. The Internet's wide range of information search and retrieval technologies, which make it possible to quickly find a vast array of information, also make it easy to access, disseminate, and trade pornographic images and videos, including child pornography. Increasingly, child pornography is accessible through Web sites, chat rooms, newsgroups, and the increasingly popular peer-to-peer technology, which allows direct communication between computer users, so that they can access and share each other's files (including images, video, and software).

As requested, our objectives were to determine (1) the ease of access to child pornography on peer-to-peer networks; (2) the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, including child pornography; and (3) the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks.

To address the first two objectives, we were assisted by the U.S. Customs CyberSmuggling Center in using a peer-to-peer application to search for image files matching keywords that were intended to identify pornography and child pornography images or that might accidentally identify pornographic images. The resulting files were downloaded, saved, analyzed, and classified by a U.S. Customs CyberSmuggling agent.¹ To determine what federal law enforcement resources are allocated to combating child pornography on peer-to-peer networks, we analyzed

¹Because child pornography cannot be accessed legally other than by law enforcement agencies, we relied on Customs to download and analyze image files. We performed analyses based on titles and file names only.

resource allocation data at the Federal Bureau of Investigation and the Child Exploitation and Obscenity Section within the Department of Justice, and at the U.S. Customs Service and U.S. Secret Service within the Department of the Treasury. We also received documentation about what resources were being allocated to combat child pornography from the National Center for Missing and Exploited Children, a federally funded nonprofit organization that serves as a national resource center for information related to crimes against children.

Appendix I contains a more detailed discussion of our objectives, scope, and methodology. Appendix II provides more information on the characteristics and use of peer-to-peer file-sharing programs.

Results in Brief

Child pornography is easily accessed and downloaded from peer-to-peer networks. Using KaZaA, a popular peer-to-peer file-sharing program, we used 12 keywords known to be associated with child pornography on the Internet to search for child pornography image files. We identified 1,286 items, each with a title and file name, determining that 543 (about 42 percent) were associated with child pornography images. Of the remaining, 34 percent were classified as adult pornography and 24 percent as nonpornographic. In another search using three keywords, the Customs CyberSmuggling Center also used KaZaA to search for and download child pornography image files.² This search identified 341 image files, of which 149 (about 44 percent) were classified as child pornography.³ The remaining images were classified as child erotica⁴ (13 percent), adult pornography (29 percent), or other (nonpornographic) images (14 percent). These results are consistent with observations of the National Center for Missing and Exploited Children, which has stated that peer-to-peer technology is increasingly popular for the dissemination of child pornography. Although peer-to-peer networks are currently not the most prominent source for child pornography, law enforcement agencies have noted a significant increase in their use for this purpose. Since 2001, when the center began to track peer-to-peer child pornography, peer-to-peer

²Other popular peer-to-peer applications include Gnutella, BearShare, LimeWire, and Morpheus.

³Customs downloaded and analyzed image files for us because child pornography can be legally accessed only by law enforcement agencies.

⁴Erotic images of children that do not depict sexually explicit conduct.

reports have increased more than fourfold—from 156 in 2001 to 757 in 2002.

When searching and downloading images on peer-to-peer networks, juvenile users face a significant risk of inadvertent exposure to pornography, including child pornography. Searches on innocuous keywords likely to be used by juveniles produce images of which a high proportion are pornographic: in our searches, the retrieved images included adult pornography (34 percent), cartoon pornography⁵ (14 percent), child erotica (7 percent), and child pornography (1 percent).

We were unable to determine the precise extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks. While several law enforcement agencies—including the Federal Bureau of Investigation, Justice’s Child Exploitation and Obscenity Section, and Customs—devote resources to combating child exploitation and child pornography in general, they do not track the resources dedicated to specific technologies used to access and download child pornography on the Internet. Therefore, we were unable to quantify the resources devoted to investigations of peer-to-peer networking. Law enforcement officials told us, however, that as they receive larger numbers of tips concerning child pornography on peer-to-peer networks, they are focusing more law enforcement resources in this area.

In commenting on a draft of this report, the Department of Justice agreed with the report’s findings and provided some additional information; Justice’s comments are reprinted in appendix III. We also received technical comments from the U.S. Secret Service and the U.S. Customs Service. Their comments have been incorporated in the report as appropriate.

Background

Federal statutes provide for civil and criminal penalties for the production, advertising, possession, receipt, distribution, and sale of child pornography.⁶ Of particular relevance to this report, the child pornography statutes prohibit the use of any means of interstate or foreign commerce (which will typically include the use of an interactive computer service) to sell, advertise, distribute, receive, or possess child pornography.

⁵Images of cartoon characters depicting sexually explicit conduct.

⁶See chapter 110 of Title 18, U.S. Code.

Additionally, federal obscenity statutes prohibit the use of any means of interstate or foreign commerce or an interactive computer service to import, transport, or distribute obscene material or to transfer obscene material to persons under the age of 16.⁷

Child pornography is defined by statute as the visual depiction of a minor—a person under 18 years of age—engaged in sexually explicit conduct.⁸ By contrast, for material to be defined as obscene depends on whether an average person, applying contemporary community standards, would interpret the work—including images—to appeal to the prurient interest and to be patently offensive, and whether a reasonable person would find the material lacks serious literary, artistic, political, or scientific value.⁹

In addition to making it a crime to transport, receive, sell, distribute, advertise, or possess child pornography in interstate or foreign commerce, federal child pornography statutes prohibit, among other things, the use of a minor in producing pornography, and they provide for criminal and civil forfeiture of real and personal property used in making child pornography and of the profits of child pornography.¹⁰ Child pornography, which is intrinsically related to the sexual abuse of children, is unprotected by the First Amendment.¹¹ Nor does the First Amendment protect the production, distribution, or transfer of obscene material.¹²

⁷See chapter 71 of Title 18, U.S. Code.

⁸See 18 U.S.C. § 2256(8).

⁹See *Miller v. California*, 413 U.S. 15 (1973). In *Miller*, the Supreme Court created a three-part test to determine whether a work is obscene. The *Miller* test, as interpreted by subsequent Supreme Court jurisprudence, asks (a) whether an average person applying contemporary community standards would find that the material, taken as a whole, appeals to the prurient interest; (b) whether an average person applying contemporary community standards would find that the material depicts proscribed behavior in a patently offensive manner; and (c) whether a reasonable person would find that the material, taken as a whole, lacks serious literary, artistic, political, or scientific value. As the *Miller* test is unrelated to child pornography, it does not account for the government's compelling interest in protecting children from sexual exploitation.

¹⁰See chapter 110, Title 18, U.S. Code.

¹¹See *New York v. Ferber*, 458 U.S. 747 (1982).

¹²See *Roth v. United States*, 354 U.S. 476 (1957). In contrast, the private possession of obscenity in one's home is protected by the First Amendment. See *Stanley v. Georgia*, 394 U.S. 557 (1969).

In enacting the Child Pornography Prevention Act of 1996,¹³ Congress sought to expand the federal prohibition against child pornography from images that involve actual children to sexually explicit images that only appear to depict minors but were produced without using any real children. The act defines child pornography as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture” that “is, or appears to be, of a minor engaging in sexually explicit conduct” or is “advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.” Last year, the Supreme Court struck down this legislative attempt to ban “virtual” child pornography¹⁴ in *Ashcroft v. The Free Speech Coalition*, ruling that the expansion of the act to material that did not involve and thus harm actual children in its creation is an unconstitutional violation of free speech rights. According to government officials, this ruling may increase the difficulty faced by law enforcement agencies in prosecuting those who produce and possess child pornography. Since the government must establish that the digital images of children engaged in sexual acts are those of real children, it may be difficult to prosecute cases in which the defendants claim that the images in question are of “virtual” children.

¹³Section 121, P.L. 104-208, 110 Stat. 3009-26.

¹⁴According to the Justice Department, rapidly advancing technology has raised the possibility of creating images of child pornography without the use of a real child (“virtual” child pornography). Totally virtual creations would be both time intensive and, for now, prohibitively costly to produce. However, the technology has led to a ready defense (the “virtual” porn defense) against prosecution under laws that are limited to sexually explicit depictions of *actual* minors. Because the technology does exist today to alter images in a manner that disguises the identity of the real child or makes the image seem computer-generated, it encourages producers and distributors of child pornography to alter depictions of actual children in slight ways to make them not only unidentifiable, but also appear as if they were virtual creations—and thereby attempt to defeat prosecution. In contrast to the weighty task of creating an entire image out of whole cloth, it is not difficult or expensive to use readily available technology to disguise depictions of real children to make them unidentifiable or to make them appear computer generated.

The Internet Has Emerged as the Principal Tool for Exchanging Child Pornography

Historically, pornography, including child pornography, tended to be found mainly in photographs, magazines, and videos.¹⁵ The arrival and the rapid expansion of the Internet and its technologies, the increased availability of broadband Internet services, advances in digital imaging technologies, and the availability of powerful digital graphic programs have brought about major changes in both the volume and the nature of available child pornography. The proliferation of child pornography on the Internet is prompting wide concern. According to a recent survey, over 90 percent of Americans say they are concerned about child pornography on the Internet, and 50 percent of Americans cite child pornography as the single most heinous crime that takes place on line.¹⁶

According to experts, pornographers have traditionally exploited—and sometimes pioneered—emerging communication technologies—from the dial-in bulletin board systems of the 1970s to the World Wide Web—to access, trade, and distribute pornography, including child pornography.¹⁷ Today, child pornography is available through virtually every Internet technology (see table 1).

¹⁵John Carr, *Theme Paper on Child Pornography for the 2nd World Congress on Commercial Sexual Exploitation of Children*, NCH Children's Charities, Children & Technology Unit (Yokohama, 2001). (http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf)

¹⁶Susannah Fox and Oliver Lewis, *Fear of Online Crime: Americans Support FBI Interception of Criminal Suspects' Email and New Laws to Protect Online Privacy*, Pew Internet & American Life Project (Apr. 2, 2001). (http://www.pewInternet.org/reports/pdfs/PIP_Fear_of_crime.pdf)

¹⁷Frederick E. Allen, "When Sex Drives Technological Innovation and Why It Has to," *American Heritage Magazine*, vol. 51, no. 5 (September 2000), p. 19. (<http://www.plannedparenthood.org/education/updatearch.html>) Allen notes that pornographers have driven the development of some of the Internet technologies, including the development of systems used to verify on-line financial transactions and that of digital watermarking technology to prevent the unauthorized use of on-line images.

Table 1: Internet Technologies Providing Access to Child Pornography

Technology	Characteristics
World Wide Web	Web sites provide on-line access to text and multimedia materials identified and accessed through the uniform resource locator (URL).
Usenet	A distributed electronic bulletin system, Usenet offers over 80,000 newsgroups, with many newsgroups dedicated to sharing of digital images.
Peer-to-peer file-sharing programs	Internet applications operating over peer-to-peer networks enable direct communication between users. Used largely for sharing of digital music, images, and video, peer-to-peer applications include BearShare, Gnutella, LimeWire, and KaZaA. KaZaA is the most popular, with over 3 million KaZaA users sharing files at any time.
E-mail	E-mail allows the transmission of messages over a network or the Internet. Users can send E-mail to a single recipient or broadcast it to multiple users. E-mail supports the delivery of attached files, including image files.
Instant messaging	Instant messaging is not a dial-up system like the telephone; it requires that both parties be on line at the same time. AOL's Instant Messenger and Microsoft's MSN Messenger and Internet Relay Chat are the major instant messaging services. Users may exchange files, including image files.
Chat and Internet Relay Chat	Chat technologies allow computer conferencing using the keyboard over the Internet between two or more people.

Source: GAO.

Among the principal channels for the distribution of child pornography are commercial Web sites, Usenet newsgroups, and peer-to-peer networks.¹⁸

Web sites. According to recent estimates, there are about 400,000 commercial pornography Web sites worldwide,¹⁹ with some of the sites selling pornographic images of children. The profitability and the worldwide reach of the child pornography trade was recently demonstrated by an international child pornography ring that included a Texas-based firm providing credit card billing and password access services for one Russian and two Indonesian child pornography Web sites.

¹⁸According to Department of Justice officials, other forums and technologies are used to disseminate pornography on the Internet. These include Web portal communities such as Yahoo! Groups and MSN Groups, as well as file servers operating on Internet Relay Chat channels.

¹⁹Dick Thornburgh and Herbert S. Lin, editors, *Youth, Pornography, and The Internet*, National Academy Press (Washington, D.C.: 2002). (http://www.nap.edu/html/youth_internet/)

According to the U.S. Postal Inspection Service, the ring grossed as much as \$1.4 million in just 1 month selling child pornography to paying customers.

Usenet. Usenet newsgroups are also providing access to pornography, with several of the image-oriented newsgroups being focused on child erotica and child pornography. These newsgroups are frequently used by commercial pornographers who post “free” images to advertise adult and child pornography available for a fee from their Web sites. The increase in the availability of child pornography in Usenet newsgroups represents a change from the mid-1990’s, when a 1995–96 study of 9,800 randomly selected images taken from 32 Usenet newsgroups found that only a small fraction of posted images contained child pornography themes.²⁰

Peer-to-peer networks. Although peer-to-peer file-sharing programs are largely known for the extensive sharing of copyrighted digital music,²¹ they are emerging as a conduit for the sharing of child pornography images and videos. A recent study by congressional staff found that one use of file-sharing programs is to exchange pornographic materials, such as adult videos.²² The study found that a single search for the term “porn” using a similar file-sharing program yielded over 25,000 files, more than 10,000 of which were video files appearing to contain pornographic images. In another study, focused on the availability of pornographic video files on peer-to-peer sharing networks, a sample of 507 pornographic video files retrieved with a file-sharing program included about 3.7 percent child pornography videos.²³

²⁰Michael D. Mehta, “Pornography in Usenet: A Study of 9,800 Randomly Selected Images,” *CyberPsychology and Behavior*, vol. 4, no. 6 (2001).

²¹According to the Yankee Group, a technology research and consulting firm, Internet users aged 14 and older downloaded 5.16 billion audio files in the United States via unlicensed file-sharing services in 2001.

²²Minority Staff, *Children’s Access to Pornography through Internet File-Sharing Programs*, Special Investigations Division, Committee on Government Reform, U.S. House of Representatives (July 27, 2001). (http://www.house.gov/reform/min/pdfs/pdf_inves/pdf_pornog_rep.pdf)

²³Michael D. Mehta, Don Best, and Nancy Poon, “Peer-to-Peer Sharing on the Internet: An Analysis of How Gnutella Networks Are Used to Distribute Pornographic Material,” *Canadian Journal of Law and Technology*, vol. 1, no. 1 (January 2002). (http://cjlt.dal.ca/vol1_no1/articles/01_01_MeBePo_gnutella.pdf)

Several Agencies Have Law Enforcement Responsibilities Regarding Child Pornography on Peer-to-Peer Networks

Table 2 shows the key national organizations and agencies that are currently involved in efforts to combat child pornography on peer-to-peer networks.

Table 2: Organizations and Agencies Involved with Peer-to-Peer Child Pornography Efforts

Agency	Unit	Focus
Nonprofit		
National Center for Missing and Exploited Children	Exploited Child Unit	Works with the Customs Service, Postal Service, and the FBI to analyze and investigate child pornography leads.
Federal entities		
Department of Justice	Federal Bureau of Investigation ^a	Proactively investigates crimes against children. Operates a national “innocent Images Initiative” to combat Internet-related sexual exploitation of children.
	Criminal Division, Child Exploitation and Obscenity Section	Is a specialized group of attorneys who, among other things, prosecute those who possess, manufacture, or distribute child pornography. Its High Tech Investigative Unit actively conducts on-line investigations to identify distributors of obscenity and child pornography.
Department of the Treasury	U.S. Customs Service CyberSmuggling Center ^a	Conducts international child pornography investigations as part of its mission to investigate international criminal activity conducted on or facilitated by the Internet.
	U.S. Secret Service ^a	Provides forensic and technical assistance in matters involving missing and sexually exploited children.

Source: GAO.

^aAgency has staff assigned to NCMEC.

The National Center for Missing and Exploited Children (NCMEC), a federally funded nonprofit organization, serves as a national resource center for information related to crimes against children. Its mission is to find missing children and prevent child victimization. The center’s Exploited Child Unit operates the CyberTipline, which receives child pornography tips provided by the public; its CyberTipline II also receives tips from Internet service providers. The Exploited Child Unit investigates and processes tips to determine if the images in question constitute a violation of child pornography laws. The CyberTipline provides investigative leads to the Federal Bureau of Investigation (FBI), U.S. Customs, the Postal Inspection Service, and state and local law enforcement agencies. The FBI and the U.S. Customs also investigate leads from Internet service providers via the Exploited Child Unit’s

CyberTipline II. The FBI, Customs Service, Postal Inspection Service, and Secret Service have staff²⁴ assigned directly to NCMEC as analysts.

Two organizations in the Department of Justice have responsibilities regarding child pornography: the FBI and the Justice Criminal Division's Child Exploitation and Obscenity Section (CEOS).²⁵

- The FBI investigates various crimes against children, including federal child pornography crimes involving interstate or foreign commerce. It deals with violations of child pornography laws related to the production of child pornography; selling or buying children for use in child pornography; and the transportation, shipment, or distribution of child pornography by any means, including by computer.
- CEOS prosecutes child sex offenses and trafficking in women and children for sexual exploitation. Its mission includes prosecution of individuals who possess, manufacture, produce, or distribute child pornography; use the Internet to lure children to engage in prohibited sexual conduct; or traffic in women and children interstate or internationally to engage in sexually explicit conduct.

Two organizations in the Department of the Treasury have responsibilities regarding child pornography: the Customs Service²⁶ and the Secret Service.

- The Customs Service targets illegal importation and trafficking in child pornography and is the country's front line of defense in combating child pornography distributed through various channels, including the Internet. Customs is involved in cases with international links, focusing on pornography that enters the United States from foreign countries. The Customs CyberSmuggling Center has the lead in the investigation of international and domestic criminal activities conducted on or facilitated by the Internet, including the sharing and distribution of child pornography on peer-to-peer networks. Customs maintains a reporting

²⁴In commenting on our report, the Secret Service noted that its staff assigned to NCMEC include analysts and an agent.

²⁵Two additional Justice agencies are involved in combating child pornography: the U.S. Attorneys Offices and the Office of Juvenile Justice and Delinquency Prevention. The 94 U.S. Attorneys Offices can prosecute federal child exploitation-related cases; the Office of Juvenile Justice and Delinquency Prevention funds the Internet Crimes Against Children Task Force Program, which encourages multijurisdictional and multiagency responses to crimes against children involving the Internet.

²⁶Under the Homeland Security Act of 2002, the Customs Service is to become part of the new Department of Homeland Security.

link with NCMEC, and it acts on tips received via the CyberTipline from callers reporting instances of child pornography on Web sites, Usenet newsgroups, chat rooms, or the computers of users of peer-to-peer networks. The center also investigates leads from Internet service providers via the Exploited Child Unit's CyberTipline II.

- The U.S. Secret Service does not investigate child pornography cases on peer-to-peer networks; however, it does provide forensic and technical support to NCMEC, as well as to state and local agencies involved in cases of missing and exploited children.

In November 2002, we reported that federal agencies are effectively coordinating their efforts to combat child pornography, and we recommended that the Attorney General designate the Postal Inspection Service and Secret Service as agencies that should receive reports and tips of child pornography under the Protection of Children from Sexual Predators Act of 1998 in addition to the FBI and Customs.²⁷

The Department of Justice, while agreeing with our finding that federal agencies have mechanisms in place to coordinate their efforts, did not fully support our conclusion and recommendation that federal coordination efforts would be further enhanced if the Postal Inspection Service and the Secret Service were provided direct access to tips reported to NCMEC by remote computing service and electronic communication service providers. Justice said that the FBI and Customs, the agencies that currently have direct access, can and do share these tips with the Secret Service and the Postal Inspection Service, as appropriate, and Justice believes that this coordination has been effective. Justice questioned whether coordination would be further enhanced by having the Secret Service and the Postal Inspection Service designated to receive access to these tips directly from NCMEC; however, Justice said that it is studying this issue as it finalizes regulations implementing the statute.

Peer-to-Peer Applications Provide Easy Access to Child Pornography

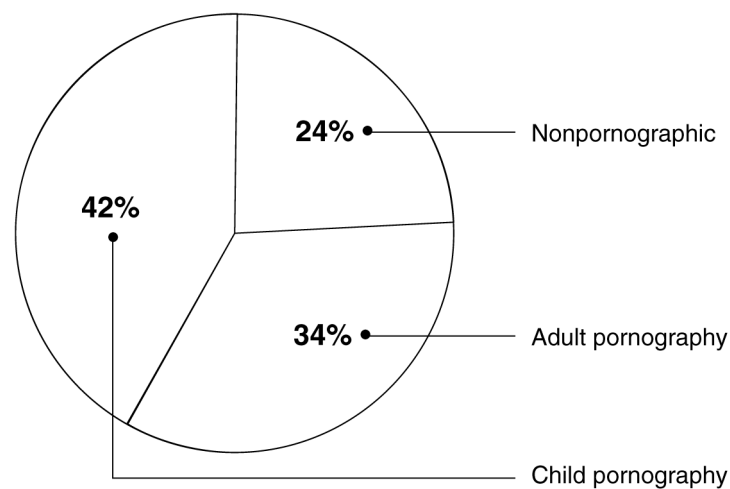
Child pornography is easily shared and accessed through peer-to-peer file-sharing programs. Our analysis of 1,286 titles and file names identified through KaZaA searches on 12 keywords²⁸ showed that 543 (about 42 percent) of the images had titles and file names associated with child

²⁷U.S. General Accounting Office, *Combating Child Pornography: Federal Agencies Coordinate Law Enforcement Efforts, but an Opportunity Exists for Further Enhancements*, [GAO-03-272](#) (Washington, D.C.: Nov. 29, 2002).

²⁸The 12 keywords were provided by the Cybersmuggling Center as examples known to be associated with child pornography on the Internet.

pornography images.²⁹ Of the remaining files, 34 percent were classified as adult pornography, and 24 percent as nonpornographic (see fig. 1). No files were downloaded for this analysis.

Figure 1: Classification of 1,286 Titles and File Names of Images Identified in KaZaA Search



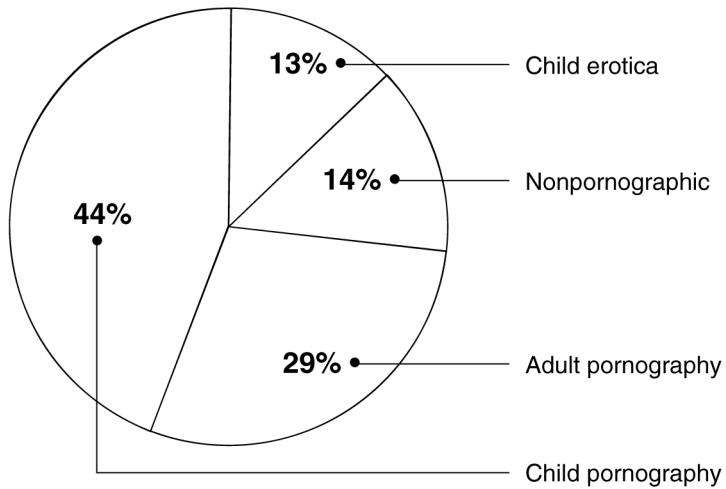
Source: GAO.

The ease of access to child pornography files was further documented by retrieval and analysis of image files, performed on our behalf by the Customs CyberSmuggling Center. Using 3 of the 12 keywords that we used to document the availability of child pornography files, a CyberSmuggling Center analyst used KaZaA to search, identify, and download 305 files, including files containing multiple images and duplicates. The analyst was able to download 341 images from the 305 files identified through the KaZaA search.

The CyberSmuggling Center analysis of the 341 downloaded images showed that 149 (about 44 percent) of the downloaded images contained child pornography (see fig. 2). The center classified the remaining images as child erotica (13 percent), adult pornography (29 percent), or nonpornographic (14 percent).

²⁹We categorized a file as child pornography if one keyword indicating a minor and one word with a sexual connotation occurred in either the title or file name. Files with sexual connotation in title or name but without age indicators were classified as adult pornography.

Figure 2: Classification of 341 Images Downloaded through KaZaA



Source: Customs CyberSmuggling Center.

Note: GAO analysis of data provided by the Customs CyberSmuggling Center.

These results are consistent with the observations of NCMEC, which has stated that peer-to-peer technology is increasingly popular for the dissemination of child pornography. However, it is not the most prominent source for child pornography. As shown in table 3, since 1998, most of the child pornography referred by the public to the CyberTipline was found on Internet Web sites. Since 1998, the center has received over 76,000 reports of child pornography, of which 77 percent concerned Web sites, and only 1 percent concerned peer-to-peer networks. Web site referrals have grown from about 1,400 in 1998 to over 26,000 in 2002—or about a nineteenfold increase. NCMEC did not track peer-to-peer referrals until 2001. In 2002, peer-to-peer referrals increased more than fourfold, from 156 to 757, reflecting the increased popularity of file-sharing programs.

Table 3: NCMEC CyberTipline Referrals to Law Enforcement Agencies, Fiscal Years 1998–2002

Technology	Number of tips				
	1998	1999	2000	2001	2002
Web sites	1,393	3,830	10,629	18,052	26,759
E-mail	117	165	120	1,128	6,245
Peer-to-peer	—	—	—	156	757
Usenet newsgroups & bulletin boards	531	987	731	990	993
Unknown	90	258	260	430	612
Chat rooms	155	256	176	125	234
Instant Messaging	27	47	50	80	53
File Transfer Protocol	25	26	58	64	23
Total	2,338	5,569	12,024	21,025	35,676

Source: Exploited Child Unit, National Center for Missing and Exploited Children.

Juvenile Users of Peer-to-Peer Applications May Be Inadvertently Exposed to Pornography

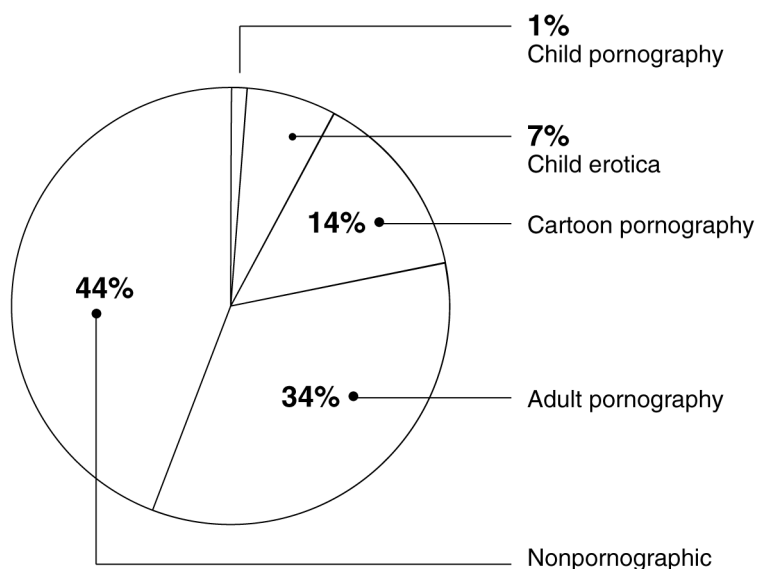
Juvenile users of peer-to-peer networks face a significant risk of inadvertent exposure to pornography when searching and downloading images. In a search using innocuous keywords likely to be used by juveniles searching peer-to-peer networks (such as names of popular singers, actors, and cartoon characters), almost half of the images downloaded were classified as adult or cartoon pornography. Juvenile users may also be inadvertently exposed to child pornography through such searches, but the risk of such exposure is smaller than that of exposure to pornography in general.

To document the risk of inadvertent exposure of juvenile users to pornography, the Customs CyberSmuggling Center performed KaZaA searches using innocuous keywords that would likely be used by juveniles. The center image searches used three keywords representing the names of a popular female singer, child actors, and a cartoon character. A center analyst performed the search, retrieval, and analysis of the images, each of which was classified into one of five categories: child pornography, child erotica, adult pornography, cartoon pornography, or nonpornographic. The searches produced 157 files, some of which were duplicates. The analyst was able to download 177 images from the 157 files identified through the search.

As shown in figure 3, our analysis of the CyberSmuggling Center’s classification of the 177 downloaded images determined that 61 images contained adult pornography (34 percent), 24 images consisted of cartoon

pornography (14 percent), 13 images contained child erotica (7 percent), and 2 images (1 percent) contained child pornography. The remaining 77 images were classified as nonpornographic.

Figure 3: Classification of 177 Images of a Popular Singer, Child Actors, and a Cartoon Character Downloaded through KaZaA



Source: Customs CyberSmuggling Center.

Note: GAO analysis of data provided by the Customs CyberSmuggling Center.

Federal Law Enforcement Agencies Are Beginning to Focus Resources on Child Pornography on Peer-to-Peer Networks

Because law enforcement agencies do not track the resources dedicated to specific technologies used to access and download child pornography on the Internet, we were unable to quantify the resources devoted to investigations concerning peer-to-peer networks. These agencies (including the FBI, CEOS, and Customs) do devote significant resources to combating child exploitation and child pornography in general. Law enforcement officials told us, however, that as tips concerning child pornography on the peer-to-peer networks increase, they are beginning to focus more law enforcement resources on this issue.

In fiscal year 2002, the key organizations involved in combating child pornography on peer-to-peer networks reported the following levels of funding:

-
- NCMEC received about \$12 million for its congressionally mandated role as the national resource center and clearinghouse. NCMEC also received about \$10 million for law enforcement training and about \$3.3 million for the Exploited Child Unit and the promotion of its CyberTipline. From the appropriated amounts, NCMEC allocated \$916,000 to combat child pornography and referred 913 tips concerning peer-to-peer networks to law enforcement agencies.
 - The FBI allocated \$38.2 million and 228 agents and support personnel to combat child pornography through its Innocent Images unit. Since fiscal year 1996, the Innocent Image National Initiative opened 7,067 cases, obtained 1,811 indictments, performed 1,886 arrests, and secured 1,850 convictions or pretrial diversions in child pornography cases. According to FBI officials, they are aware of the use of peer-to-peer networks to disseminate child pornography and have efforts under way to work with some of the peer-to-peer companies to solicit their cooperation in dealing with this issue.
 - CEOS allocated \$4.38 million and 28 personnel to combat child exploitation and obscenity offenses. It has recently launched an effort, the High Tech Investigative Unit, dealing with investigating any Internet medium that distributes child pornography, including peer-to-peer networks.
 - Customs allocated \$15.6 million and over 144,000 hours to combating child exploitation and obscenity offenses.³⁰ The CyberSmuggling Center is beginning to actively monitor the file sharing of child pornography on peer-to-peer networks and is devoting one half-time investigator to this effort. As of December 16, 2002, the center has sent 21 peer-to-peer investigative leads to the field offices for follow-up action. Four of these leads have search warrants pending, two have been referred to local law enforcement, and five have been referred to foreign law enforcement agencies.

In addition, to facilitate the identification of the victims of child pornographers, the CyberSmuggling Center is devoting resources to the National Child Victim Identification Program, a consolidated information system containing seized images that is designed to allow law enforcement officials to quickly identify and combat the current abuse of children associated with the production of child pornography. The system's database is being populated with all known and unique child pornographic images obtained from national and international law enforcement sources

³⁰Customs is unable to separate the staff hours devoted or funds obligated to combating child pornography from those dedicated to combating child exploitation in general.

and from CyberTipline reports filed with NCMEC. It will initially hold over 100,000 images that have been collected by federal law enforcement agencies from various sources, including old child pornography magazines.³¹ According to Customs officials, this information will help, among other things, to determine whether actual children were used to produce child pornography images by matching them with images of children from magazines published before modern imaging technology was invented. Such evidence can be used to counter the assertion that only virtual children appear in certain images.

The system is housed at the Customs CyberSmuggling Center and is to be accessed remotely in “read only” format by the FBI, CEOS, the U.S. Postal Inspection Service, and NCMEC. An initial version of the system was deployed at the Customs CyberSmuggling Center in September 2002; the system became operational in January 2003.³²

Conclusions

It is easy to access and download child pornography on peer-to-peer networks. Juvenile users of peer-to-peer networks also face a significant risk of inadvertent exposure to pornography, including child pornography. We were unable to determine the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks; the key law enforcement agencies devote resources to combating child exploitation and child pornography in general, but they do not track the resources dedicated to peer-to-peer technologies in particular.

Agency Comments and Our Evaluation

The Assistant Attorney General, Criminal Division, Department of Justice, provided written comments on a draft of this report, which are reprinted in appendix III. The Department of Justice agreed with the report’s findings, provided additional information on the mission and capabilities of the High Tech Investigative Unit (part of its Criminal Division’s Child Exploitation and Obscenity Section), and offered comments on the description and purpose of Customs’ National Child Victim Identification

³¹According to federal law enforcement agencies, most of the child pornography published before 1970 has been digitized and made widely available on the Internet.

³²One million dollars has already been spent on the system, with an additional \$5 million needed for additional hardware, the expansion of the image database, and access for all involved agencies. The 10-year lifecycle cost of the system is estimated to be \$23 million.

Program. In response, we have revised our report to add these clarifications. We also received written technical comments from the Department of Justice, which we have incorporated as appropriate.

We received written technical comments from the Assistant Director, Office of Inspection, U.S. Secret Service, and from the Acting Director, Office of Planning, U.S. Customs Service. Their comments have been incorporated in the report as appropriate.

As agreed with your office, 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 the Departments of Justice and the Treasury. We will also send copies to the Attorney General and to the Secretary of the Treasury. 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 be also reached by E-mail at koontzl@gao.gov and dolakm@gao.gov, respectively. Key contributors to this report were Barbara S. Collier, James M. Lager, Neelaxi V. Lakhmani, James R. Sweetman, Jr., and Jessie Thomas.



Linda D. Koontz
Director, Information Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to

- determine the ease of access to child pornography on peer-to-peer networks,
- assess the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, including child pornography, and
- determine the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks.

To determine the availability of child pornography on peer-to-peer networks, we used a popular peer-to-peer application—KaZaA—to search for and identify image files that appear to be child pornography. Our analysts used keywords provided by the Customs CyberSmuggling Center. These keywords were intended to identify pornographic images; examples of the keywords include *preteen*, *underage*, and *incest*.

Once the names and titles of image files were gathered, we classified and analyzed them based on file names and keywords. Each file was classified as child pornography, adult pornography, or nonpornographic. For a file to be considered possible child pornography, the title, file name, or both had to include at least one word with a sexual connotation and an age-related keyword indicating that the subject is a minor. Files depicting adult pornography included any file that had words of a sexual nature in the title or file name. No files were downloaded for this analysis.

To determine the ease of access, we used three keywords from the initial list to perform another search. The resulting files were downloaded, saved, and analyzed by a Customs agent. Because child pornography cannot be accessed legally other than by law enforcement agencies, we relied on Customs to download and analyze files. Our own analyses were based on keywords and file names only. The Customs agent classified each of the downloaded files into one of four categories: child pornography, child erotica, adult pornography, or nonpornographic. The user with the largest number of shared files that appeared to be child pornography was also identified, and the shared folder was captured. The titles and names of files in the user's shared directory were then analyzed and classified by a GAO analyst using the same classification criteria used in original analysis.

To assess the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography, a CyberSmuggling Center analyst conducted another search using three keywords that are names of popular celebrities and a cartoon character. The Customs analyst performed the search, retrieval, and analysis of the images. Each of the images downloaded was

classified into one of five categories: adult pornography, child pornography, child erotica, cartoon pornography, or nonpornographic.

To determine what federal law enforcement resources were allocated to combating child pornography on peer-to-peer networks, we obtained resource allocation data and interviewed officials at the U.S. Customs Service, the Department of Justice's Child Exploitation and Obscenity Section, and the Federal Bureau of Investigation. We also received information about what resources were being allocated to combat child pornography from the U.S. Secret Service and the National Center for Missing and Exploited Children.

We performed our work between July and October 2002 at the U.S. Secret Service in Baltimore, Maryland, and the U.S. Customs Service, Customs CyberSmuggling Center, in Fairfax, Virginia, under the Department of the Treasury; and at the Child Exploitation and Obscenity Section and the Federal Bureau of Investigation, under the Department of Justice, in Washington, D.C. We also worked with the National Center for Missing and Exploited Children in Alexandria, Virginia. Our work was conducted in accordance with generally accepted government auditing standards.

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 traditional model, the peer-to-peer model enables consenting users—or peers—to directly interact and share information with each other 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 built around this model.³ These range from the SETI@home network (where users share the computing power of their computers to search for extraterrestrial life) to the popular KaZaA file-sharing program (used to share music and other files).

As shown in figure 4,⁴ 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

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). (people.cs.uchicago.edu/~matei/PAPERS/ic.pdf)

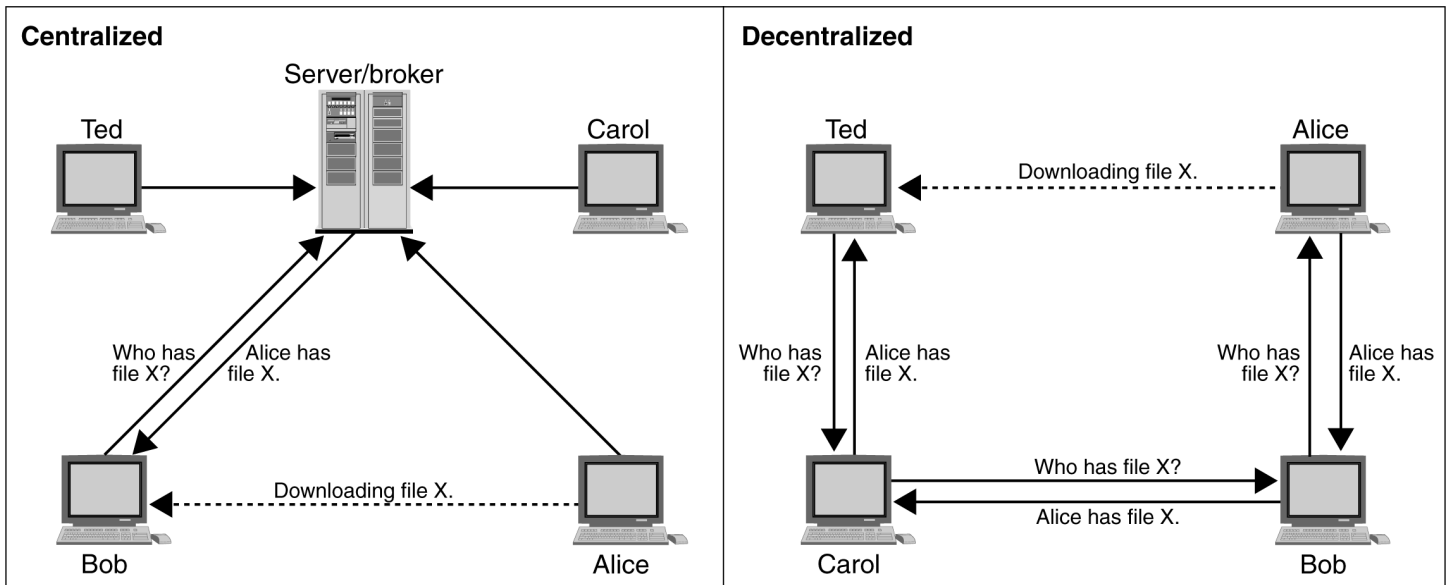
²Zeropaid.com, a file-sharing portal, lists 88 different peer-to-peer file-sharing programs available for download. (<http://www.zeropaid.com/php/filessharing.php>)

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)

⁴Illustration 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).

model, based on the Gnutella⁵ network, in which individuals find and interact directly with each other.

Figure 4: Peer-to-Peer Models



Source: Mark Bontrager, Bob Knighten.

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

As shown in figure 4, 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 Bob submits a request for a particular 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 Bob, who can then select the desired file from the list and open a direct link with Alice's computer, which currently has the file. The download of the actual file takes place directly from Alice to Bob.

⁵According 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 AOL 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>)

The broker model was used by Napster, the original peer-to-peer network, facilitating 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 challenges⁶ 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 service, so, according to Gartner,⁷ 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, Ted starts with a networked computer equipped with a Gnutella file-sharing program, such as KaZaA or BearShare. Ted connects to Carol, Carol to Bob, Bob to Alice, and so on. Once Ted'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 Carol, who will each in turn send the request to the computers to which they are connected, and so forth. If one of the computers in the peer network (say, for example, Alice's) has a file that matches the request, it transmits the file information (name, size, type, etc.) back through all the computers in the pathway towards Ted, where a list of files matching the search request appears on Ted's computer through the file-sharing program. Ted will then be able to open a connection with Alice and download the file directly from Alice's computer.⁸

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 (VNS). A VNS dynamically associates user-created names with the Internet address of whatever Internet-connected computer users happen to be

⁶*A&M Records v. Napster*, 114 F.Supp.2d 896 (N.D. Cal. 2000).

⁷Lydia Leong, "RIAA vs. Verizon, Implications for ISPs," Gartner (Oct. 24, 2002).

⁸LimeWire, *Modern Peer-to-Peer File Sharing over the Internet*.
(<http://www.limewire.com/index.jsp/p2p>)

using when they log on.⁹ The VNS facilitates point-to-point interaction between individuals, because it removes the need for users and their computers to know the addresses and locations of other users; the VNS can, to certain extent, preserve users' anonymity and provide information on whether a user is or is not connected to the Internet at a given moment.¹⁰

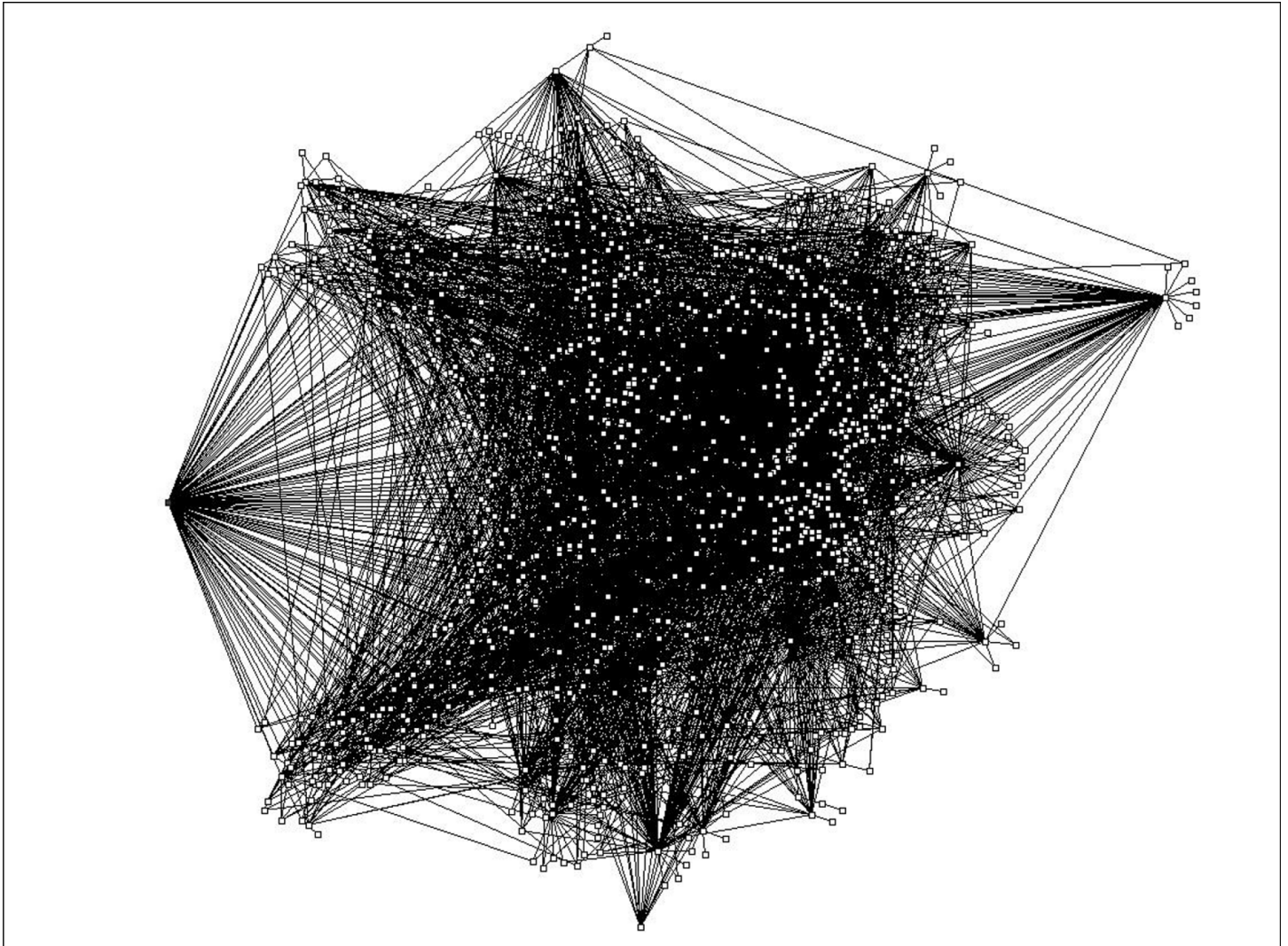
The file-sharing networks that result from the use of peer-to-peer technology are both extensive and complex. Figure 5 shows a map or topology of a Gnutella network whose connections were mapped by a network visualization tool.¹¹ The map, created in December 2000, shows 1,026 nodes (computers connected 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.

⁹S. Hayward and R. Batchelder, "Peer-to-Peer: Something Old, Something New," Gartner (Apr. 10, 2001).

¹⁰Peer-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.

¹¹Mihajlo 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 5: 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: Comments from the Department of Justice



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

February 3, 2003

Ms. Linda D. Koontz
Director
Information Management Issues
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Koontz:

The Department of Justice has reviewed the GAO proposed report entitled, "File Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography" (GAO-03-351) (the "Proposed Report"). We agree with the Proposed Report's findings that child pornography is readily available on peer-to-peer networks, that juveniles using such networks may be inadvertently exposed to child pornography as well as other pornographic material, and that federal law enforcement agencies are devoting substantial resources to fighting child exploitation and child pornography. We also would like to express our appreciation to GAO for its effort in conducting a careful, thorough, and diligent study of this important issue, and for its recognition that the Criminal Division's Child Exploitation and Obscenity Section ("CEOS") has taken an important role in combating child exploitation and child pornography.

While we support the Proposed Report's findings, we offer, as important additional context, the information set forth below describing the Department's innovative approach to meeting and anticipating the latest technology challenges and explaining, in greater detail, the full scope of the National Child Victim Identification Program.

Understanding that child pornographers are increasingly mastering and using cutting-edge technology to commit their crimes and avoid apprehension, and understanding the existence of a technology gap between law enforcement generally and the offenders, CEOS created a High Tech Investigative Unit (HTIU) within CEOS, staffed with computer forensic experts, to keep pace with misused technology and to fill that gap. The goal of the HTIU is to ensure that

Internet-based child pornography and adult obscenity prosecutions benefit from the special expertise brought to bear by technology experts. HTIU's computer forensic specialists can and do meet the challenge presented by the use of peer-to-peer networks in the commission of child pornography and adult obscenity crimes. More importantly, the Unit is poised to meet new technological challenges that will surely develop as technology evolves.

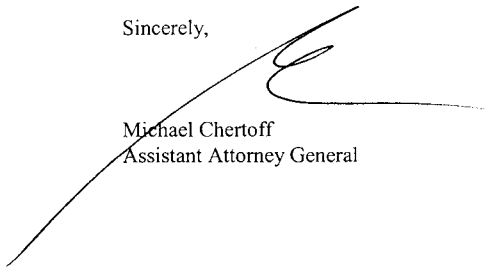
The National Child Victim Identification Program (NCVIP), discussed in the Proposed Report, exemplifies the cooperative mind-set that exists in the law enforcement community in addressing child pornography and child abuse crimes effectively and decisively. The NCVIP also exemplifies the cooperative mind-set that exists between the law enforcement community and private organizations to marshal every resource, public or private, to eradicate the trade in child pornography, identify current abuse, and bring the perpetrators to justice.

The Proposed Report characterizes the NCVIP as an "information system and database of child pornography images" intended to "help determine whether actual children were used to produce child pornography images by matching them with images of children from magazines published before modern imaging technology was invented." Proposed Report, at 16. While this description exemplifies one part of the NCVIP's design, it does not adequately explain that the NCVIP is primarily intended to help law enforcement identify and stop *current* instances of child abuse associated with the production of child pornography. The NCVIP will help stop *current* child abuse by allowing law enforcement, upon discovering an image of child pornography, quickly to determine whether that image is new or dated. If the image is new, law enforcement can then take steps to identify the victim and the producer with the goal of preventing continued abuse of the victim. For far too long, law enforcement's focus has been on the image itself – with little consideration for the serious abuse depicted in the images. The lack of focus on the abuse represented in the images stemmed mostly from the fact that investigators had no means of determining whether the abuse depicted was recent or current, or many years old. NCVIP will be instrumental in focusing law enforcement's efforts on current abuse and ensuring that our focus is not simply limited to the trafficking of child pornographic images, but extends to the investigation and prosecution of the underlying abuse. Accordingly, we recommend that the proposed report describe the NCVIP as primarily "a consolidated information system containing seized images of child pornography designed to allow law enforcement quickly to identify and combat the current abuse of children associated with the production of child pornography."

In sum, we agree that those who engage in the production and trafficking of child pornography are consistently early adopters of emerging technologies. The Department has risen to, and met, that challenge by ensuring an equal or greater level of technological expertise on the part of its prosecutors and agents investigating Internet-based child pornography and adult obscenity crimes.

I hope you will consider our comments in preparing the final GAO report on this subject. If you have any questions regarding the Department's comments, you may contact Vickie L. Sloan, Director, Audit Liaison Office, on (202) 514-0469.

Sincerely,



Michael Chertoff
Assistant Attorney General

Glossary

Broadband	Operating at bandwidths markedly greater than that provided by telephone networks. Broadband networks can carry digital videos or a massive quantity of data simultaneously. In the on-line environment, the term is often used to refer to Internet connections provided through cable or DSL (digital subscriber line) modems.
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.
Cartoon pornography	Images of cartoon characters engaged in sexual activity.
Chat	Internet program enabling users to communicate through short written messages. Some of the most popular chat programs are America Online's Instant Messenger and the Microsoft Network Messenger. See instant messaging.
Child erotica	Sexually arousing images of children that are not considered pornographic, obscene, or offensive.
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.

Hypertext language (HTML)	The standard language (HyperText Markup Language) used to display information on the Web. It uses tags embedded in text files to encode instructions for formatting and displaying the information.
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 instant messaging service. America Online's Instant Messenger and the Microsoft Network Messenger are among the most popular instant messaging programs (see chat).
Internet relay chat (IRC)	Internet chat application allowing real-time conversations to take place via software, text commands, and channels. Unlike the Web-based IM, IRC requires special software and knowledge of technical commands (see chat).
IP address	Internet Protocol 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, free for the public to use.
Morpheus	A file-sharing application using the KaZaA peer-to-peer protocol to share files among users on the network.
Morphing	A process whereby one image is gradually transformed into a second image.
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.

Newsgroups	Discussion groups on Usenet, varying in topic from technical to bizarre. There are over 80,000 newsgroups organized by major areas or domains. The major domains are alt (any conceivable topic, including pornography); biz (business products and services); rec (games and hobbies); comp (computer hardware and software); sci (sciences); humanities (art and literature); soc (culture and social issues); misc (miscellaneous, including employment and health); and talk (debates on current issues). See Usenet.
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 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.
Usenet	A bulletin board system accessible through the Internet containing more than 80,000 newsgroups. Originally implemented in 1979, it is now probably the largest decentralized information utility in existence (see newsgroups).
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 GAO Mailing Lists" under "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

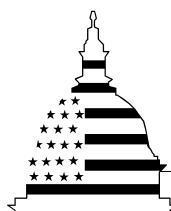
Public Affairs

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

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.

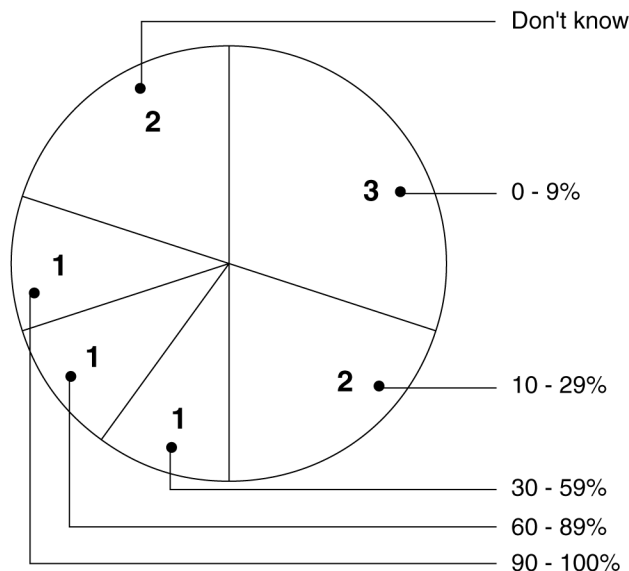
University Officials We Interviewed Are Aware of the Use of File-Sharing Applications on Their Networks

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)



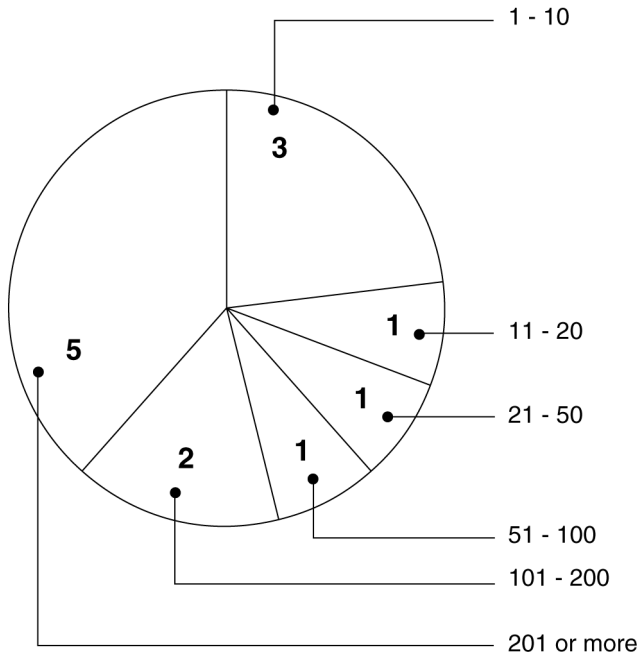
Source: GAO analysis of survey responses.

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.

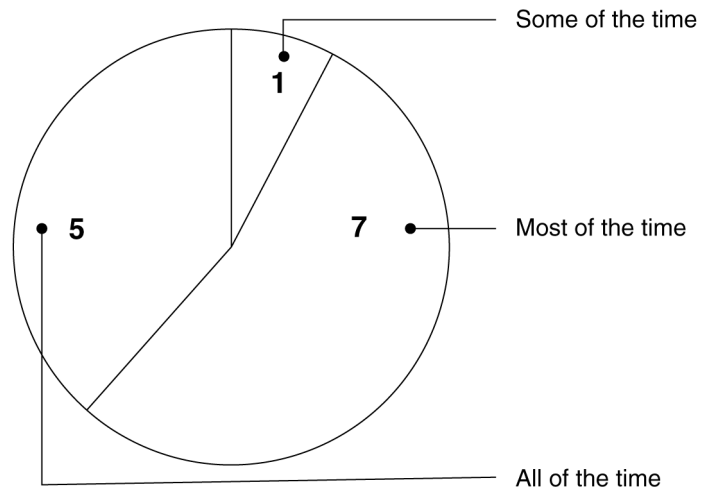
In addition, all of the college and university officials interviewed indicated that they had received notices from representatives of copyright holders alleging file-sharing copyright violations by students, with more than half of the interview respondents indicating that they had received more than 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)

How many notifications were received of alleged file sharing copyright violations by individual students



Ability of university officials to track violation notices to individual students



Source: GAO analysis of survey responses.

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

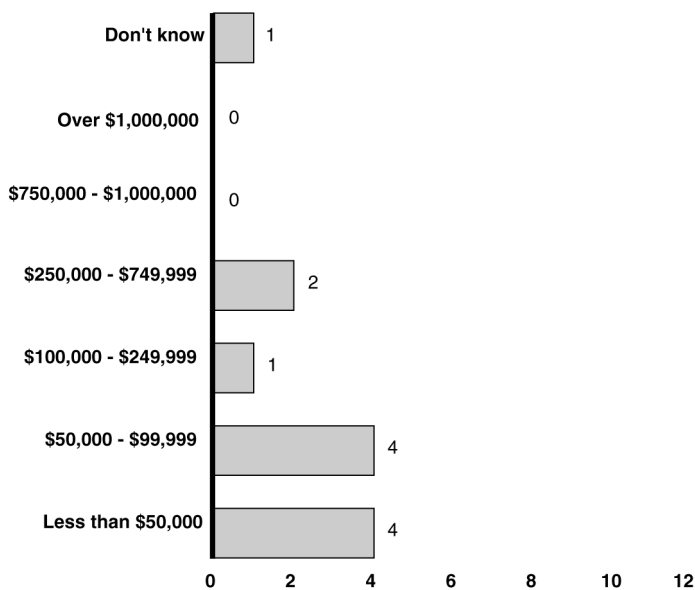
Overall, most of the college and university officials we interviewed indicated that they had experienced some network performance or security problems as a result of the use of peer-to-peer file-sharing applications on their institutions' networks. Specifically, two officials interviewed stated that 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

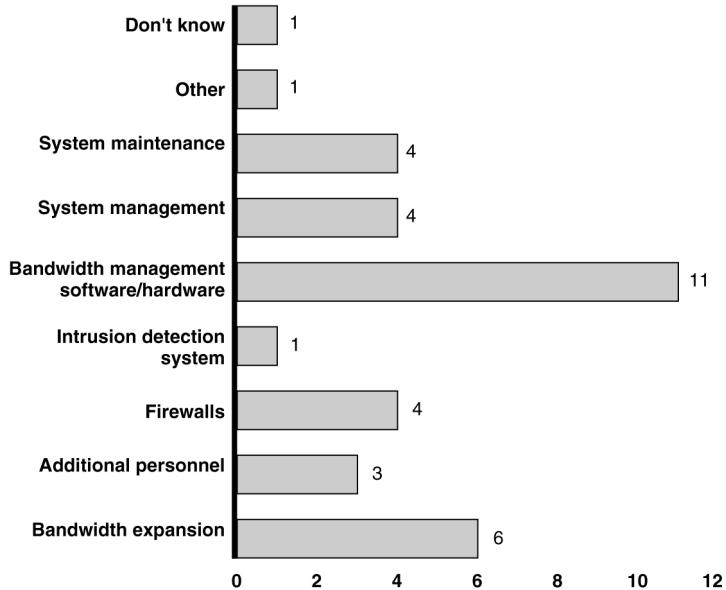
academic year to deal with the effects of the use of peer-to-peer file-sharing applications on their networks, with the median amount of additional spending being between \$50,000 and \$99,999;⁸ two officials stated that their institutions had spent between \$250,000 to \$749,999. This additional funding 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.

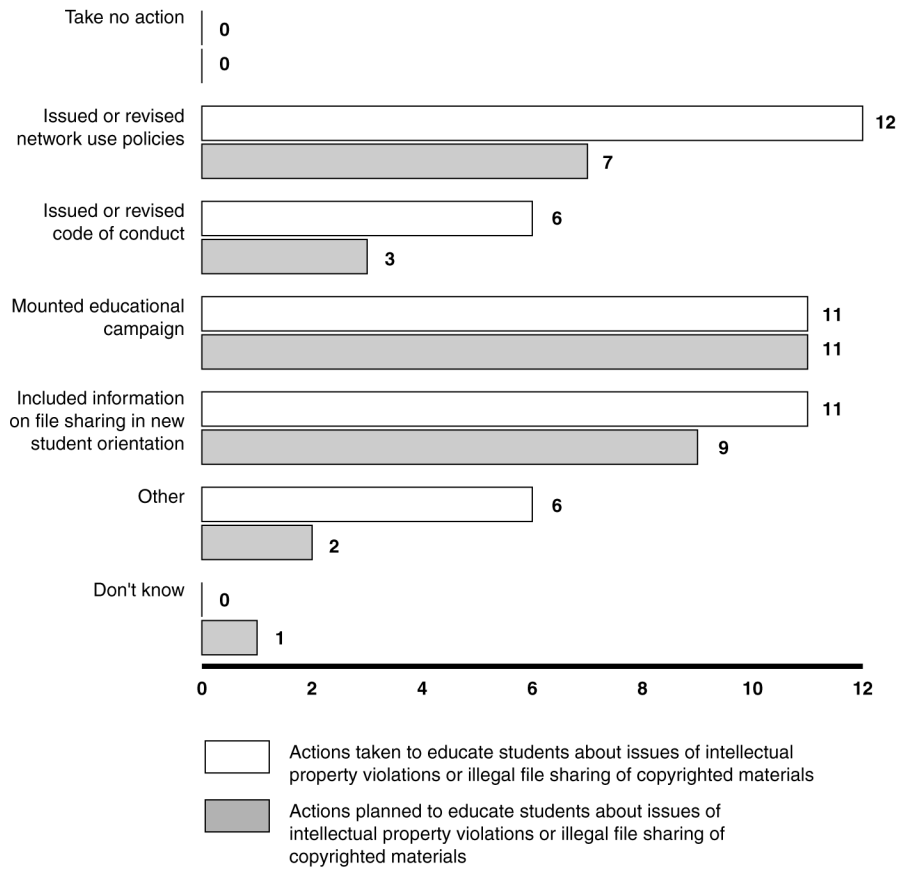
⁸A median is the value in an ordered set of values below and above which there is an equal number of values; if there is no one middle number, it is the value that is the arithmetic mean of the two middle values.

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)



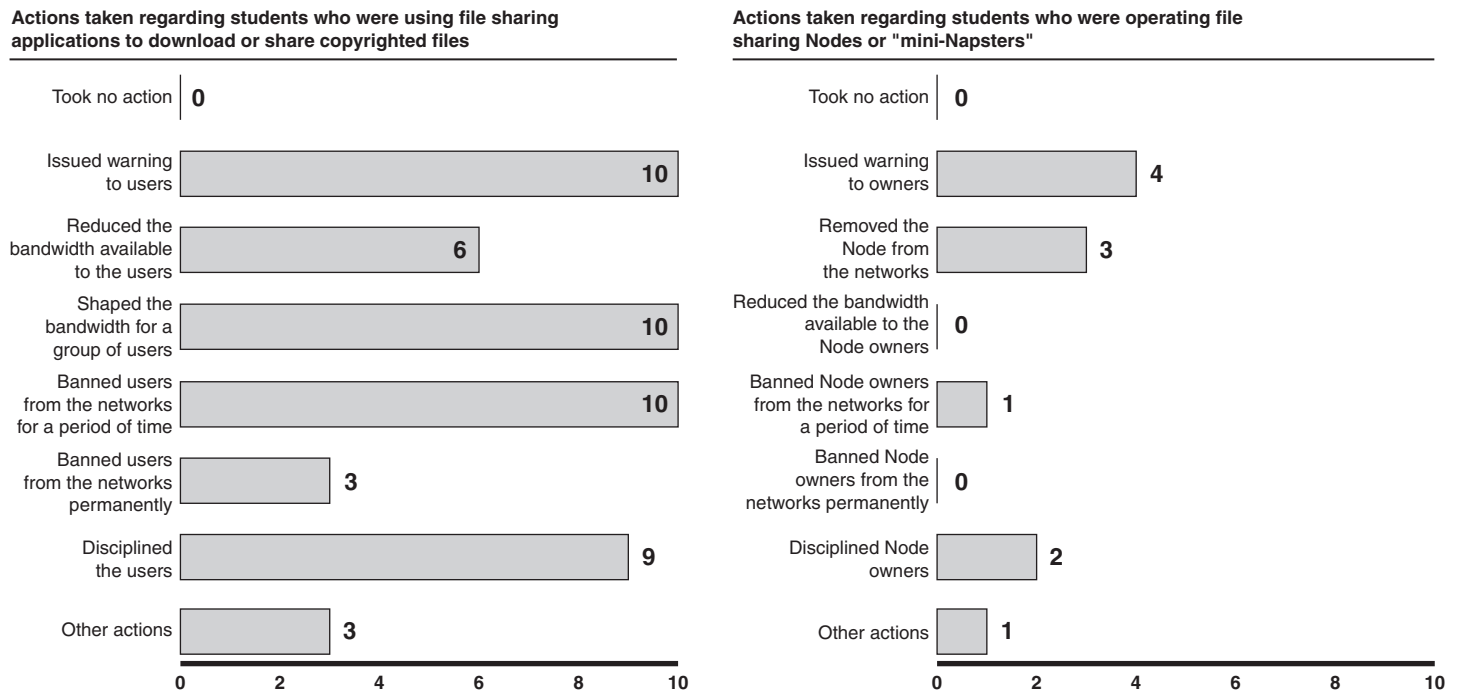
Source: GAO analysis of survey responses.

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.

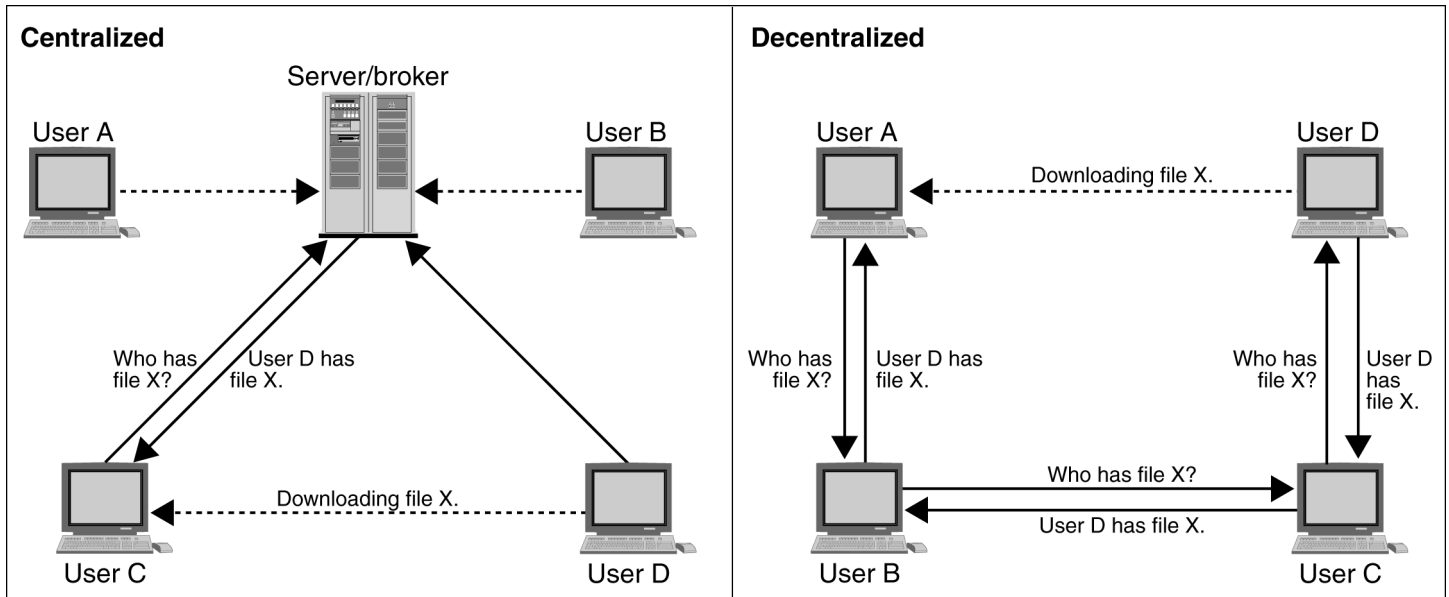
- *Collaboration applications*, which enable teams in different geographic areas to work together and increase productivity. For example, the Groove application can access data on traditional corporate networks and on nontraditional devices such as personal digital assistants and handheld devices.

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).

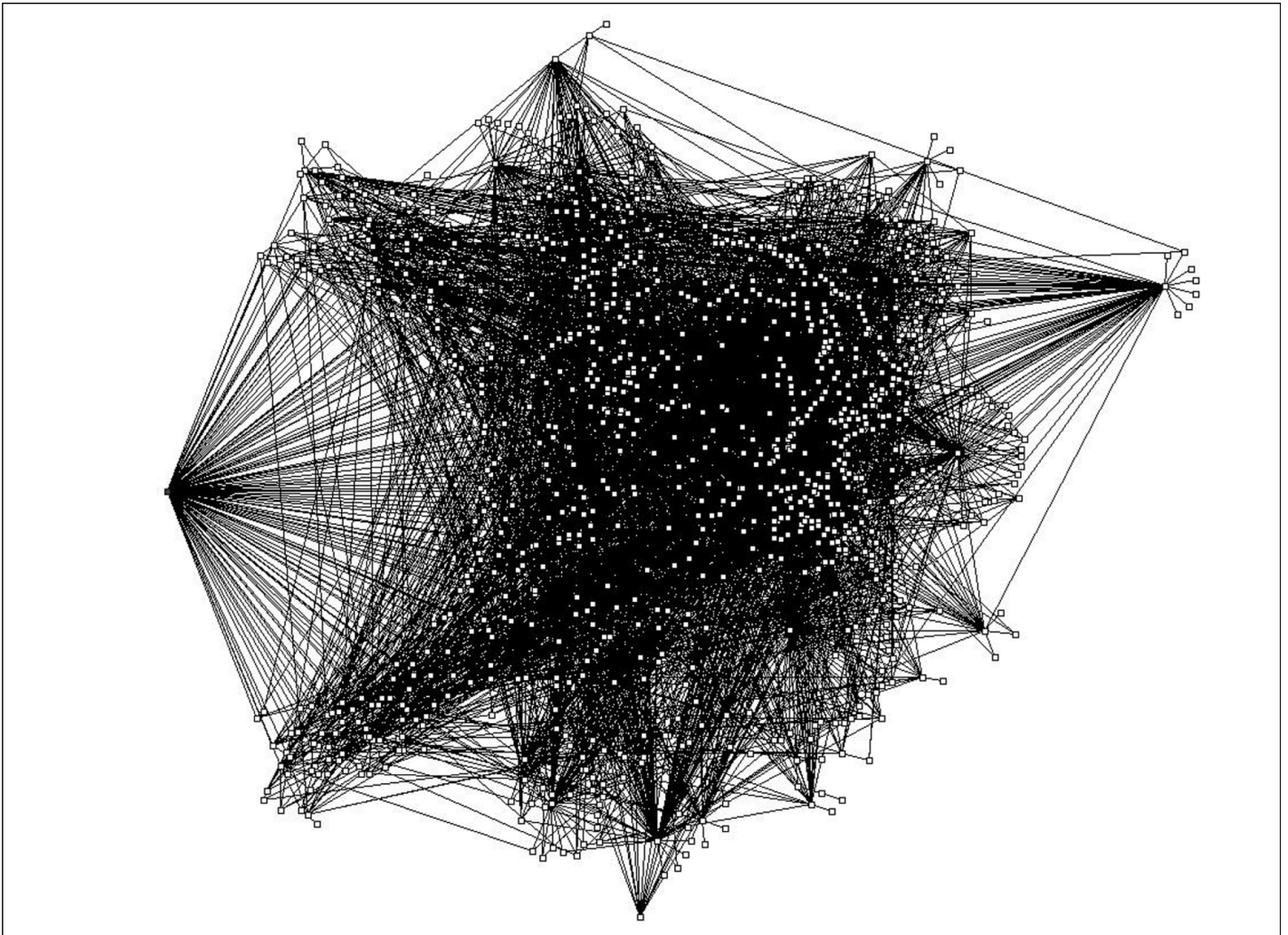
other users; the virtual name space can, to a certain extent, preserve users' anonymity and provide information on whether a user is or is not connected to the Internet at a given moment.¹¹

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.

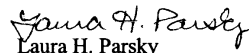
(6) statutory thresholds favor a federal criminal enforcement focus on the more sophisticated targets: the statutory thresholds require a retail value of \$2,500 or more of the goods pirated by the infringer. Consequently, if each song that is traded on a peer-to-peer application is valued at \$0.80, 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

**STATEMENT OF CARY SHERMAN
PRESIDENT, RECORDING INDUSTRY ASSOCIATION OF AMERICA
BEFORE THE
SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL
PROPERTY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES
ON
PEER-TO-PEER (P2P) PIRACY ON UNIVERSITY CAMPUSES: AN UPDATE**

OCTOBER 5, 2004

Chairman Smith, Ranking Democratic Member Berman, and Members of the Subcommittee, I appreciate this opportunity to appear before the Subcommittee today to continue our ongoing discussion of P2P piracy on campus. In particular, I gratefully acknowledge the Subcommittee's steadfast commitment to this subject, as evidenced by the fact that it was the subject of the very first hearing held in this Subcommittee this Congress. The work of this Subcommittee has been invaluable in helping us convey the message that illegal downloading on college campuses – or anywhere else – is simply not acceptable.

This past month, schools across the country have welcomed students back to a continuously evolving environment. With a casual walk across campus, it is impossible to miss the iPods and other portable music devices; with a quick visit to any dorm room, you will discover the stacks of CDs or the computers full of mp3s. Music collection and enjoyment remains a favorite pastime for students. Unfortunately, so does piracy.

We've been doing our part to address this issue. For instance, the Campus Action Network (CAN), a program led by Sony BMG and supported by other record companies, has worked to encourage and facilitate the launch of legitimate music services on campuses across the country. These services are made possible by the specialized packages and greatly discounted rates provided by the entertainment industry. The motion picture industry has also instituted a program to work with schools to address P2P piracy on campus. We are working hard to find new ways to provide the entertainment products students want and can acquire conveniently and legally. At the same time, we have reminded students that their academic status does not give them a free pass to infringe. Since March of this year, 190 students at 61 universities have been included in a series of lawsuits directed at infringers of copyrighted material on P2P networks. The message has been received loud and clear: responsibility does not wait for graduation.

We are pleased to report that schools have been doing their part as well. There is considerable good news here. As the Joint Committee of the Higher Education and Entertainment Communities reported to this subcommittee in August, colleges and universities across the country have become engaged in a variety of initiatives to stem the rampant piracy on their computer networks. Perhaps the most exciting of these initiatives have been the partnerships between schools and legitimate online services I mentioned

earlier. These agreements, jump-started by the success of a landmark deal between the now-legitimate Napster and Penn State University, have enabled college and university administrations to offer their students access to the music they desire—and, indeed, often demand—while ensuring the responsible, safe, and economic use of their network resources. To date, 25 schools have reported signing with legitimate services such as Napster, Cdigix, RealNetworks, MusicRebellion, Ruckus, and iTunes to distribute content legally and efficiently. And interest is growing exponentially. We have seen the formation of school task forces, and even student groups, to consider whether a campus-based online service is best for them. Student papers have carried editorials eagerly requesting such services at their schools. Schools have also worked to find new uses for these services, such as offering streaming and downloadable content to augment their curriculum.

The installation of these services on campuses has helped to reduce network congestion, decrease infringements, and maintain the security and integrity of the system. Schools have also turned to other technological means to curtail improper use of their networks. In addition to traditional bandwidth shaping and limits, new systems and devices are being used across the country. The University of Florida introduced ICARUS, an application that automatically prevents infringement through P2P services. UCLA implemented ACNS, an automated system that streamlines the notification of, and penalty for, copyright infringement. Audible Magic's CopySense system, which uses filtering technology to weed out infringing transmissions, has also been installed to great effect on several school networks.

Of course, education remains a fundamental component of any school's fight against P2P piracy. Recognizing their unique position to prepare students for the opportunities and responsibilities of adulthood, institutions across the country have undertaken various initiatives to inform students about copyright laws and the appropriate use of computer networks. Emails and letters have been sent to school communities by presidents and deans; tutorials and quizzes have been designed to ensure compliance with policies, laws, and standards; notices, posters, and fliers have been distributed; discussions, presentations, and courses have been held; skits, videos, and other entertaining informative pieces have been made. More and more students are not only getting the message that using their schools' resources to engage in illegal conduct is wrong, they are learning why. Copyrighted works have value and theft of these works does, indeed, cause harm. Importantly, it is this knowledge that students carry with them and apply after graduation.

Finally, messages are hitting home through enforcement. Violations of schools' acceptable use policies regularly carry penalties, and abuses of schools' computer networks are no exception. Students are increasingly aware of the frequently tiered courses of action taken after incidents of online infringement. First violations often carry warnings and brief denials of network access. Second violations often increase penalties to extended denials of network access, referrals to the Dean, and probation. Third violations, while rare, can often lead to permanent removal from the network, suspension, or, in extreme cases, even expulsion.

The combined effects of these initiatives—legitimate services, technology, education, and enforcement—have resulted in a positive change in the attitudes and responses of administrations and students.

However, with the good news comes the distinct reminder that we are not in the clear. College and university campuses remain a hotbed for piracy. Students, with limited budgets and, perhaps, misguided senses of entitlement, can unfortunately still find a treasure trove of valuable and free copyrighted works available over extremely fast and convenient computer networks.

In fact, the speed of these networks has created new challenges for copyright owners. Internet 2, a consortium of schools, industry, and government, is an exciting platform for advanced network applications and technologies. Yet, as with other networks, bad actors have begun to hijack it, threatening to turn a beneficial and promising technology into a tool for piracy. Already, P2P systems, such as i2hub, have been set up on Internet 2, facilitating the abuse of advanced networking technology to illegally distribute copyrighted works for free. The speed of these networks—up to thousands of times faster than ordinary Internet networks—allows users to obtain copyrighted movies in minutes and music in seconds. Further, the closed nature of these networks, being available only to those engaged in academia, makes it more difficult for copyright owners to protect their works and to notify responsible parties of their infringement.

The naturally high speeds of college and university networks has also allowed students to set up local area networks—or LANs—to connect with others solely within their individual schools. The RIAA brought suit last year against the student operators of four such networks, who had effectively used their school’s resources to create “mini-P2P networks” to facilitate the mass piracy of copyrighted works on their campuses. As with Internet 2, the closed nature of these LANs makes it difficult to discover such misuse. College and university administrations are in the best position to determine the pervasiveness of this LAN-based piracy, and to take action to stop it.

School administrations have been working hard to bring users of their computer networks into compliance with proper standards, laws, and acceptable use policies. But it is imperative that they do not allow loopholes in their rules and enforcement. Restrictions placed on standard Internet use should be clearly extended to new and evolving opportunities such as Internet 2 and LANs. The vigilance with which administrators ensure the integrity of their systems must continue through the introduction of these new services and technologies.

P2P piracy clearly remains a problem on college and university campuses across the country. And, undoubtedly, challenges lie ahead. Yet, the opportunities for the education and entertainment communities to work together toward a mutually beneficial end have never been as great as they are today. With the multi-pronged approach I’ve discussed here and in the Joint Committee report to this Subcommittee in August, the

future looks even brighter. We look forward to continuing our work with all interested parties and to providing increasingly positive reports in the future.

Thank you.

**PEER-TO-PEER SOFTWARE PROVIDERS' LIABILITY
UNDER SECTION 5 OF THE FTC ACT**

April 27, 2004

Howrey Simon Arnold & White, LLP
Washington, DC
Lisa Jose Fales, Esq.
Charles Webb, Esq.

The CapAnalysis Group, LLC
Washington, DC
James C. Miller III, Ph.D.
Jeffrey A. Eisenach, Ph.D.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE RISE AND MECHANICS OF P2P FILE-SHARING.....	4
	A. P2P File-Sharing Continues to Escalate	4
	B. Mechanics of P2P File-Sharing	5
III.	PROVIDERS OF P2P SOFTWARE DO NOT ADEQUATELY DISCLOSE THE RISK OF VIRUSES ON P2P NETWORKS	6
IV.	CONSUMERS ARE HARMED THROUGH P2P SOFTWARE PROVIDERS’ POTENTIALLY DECEPTIVE PRACTICES CONCERNING SPYWARE/ADWARE.....	9
	A. P2P Software Providers Fail to Adequately Disclose to Consumers the Inclusion of Spyware/Adware	11
	B. Spyware Distributed With P2P Software Compromises Consumer Privacy.....	14
	C. There are a Myriad of Additional Consumer Harms Caused by Adware/Spyware.....	17
V.	P2P PROVIDERS FAIL TO ADEQUATELY WARN USERS OF LITIGATION RISKS	18
VI.	PROVIDERS FAIL TO WARN USERS OF VIOLENT OR OFFENSIVE MATERIALS AVAILABLE THROUGH THEIR NETWORKS AND OF THE RISK OF USERS BECOMING UNWITTING DISTRIBUTORS	21
VII.	AN FTC INVESTIGATION IS WARRANTED TO DETERMINE WHETHER P2P PROVIDERS’ BUSINESS PRACTICES VIOLATE THE FTC ACT.....	22
	A. P2P Providers Have Engaged in Deceptive Representations and Failed to Disclose Material Facts.....	23
	B. FTC Enforcement Under Section 5 Would Advance Consumer Sovereignty	26
	C. P2P Providers’ Business Practices May Also Violate the Children’s Online Privacy Protection Act.....	27
VIII.	CONCLUSION.....	30

I. INTRODUCTION¹

Peer-to-peer (“P2P”) software providers, such as KaZaA, Grokster, Morpheus, and Limewire, distribute free file-sharing software to end-user consumers throughout the U.S. and the world. The P2P software enables consumers who are part of the P2P network to easily search millions of other in-network consumers’ personal folders for files, including images and videos, and to download them free of charge. The P2P providers profit by selling advertisements that appear both on their websites and on the users’ computers when they employ the file-sharing software. Some of these advertisements are generated by third-party software providers who partner with P2P software providers to bundle their software with the P2P software in exchange for a fee. Several P2P providers also profit by selling “premium” file-sharing software that is “ad free,” typically at a subscription cost to the end-user of around \$30.00.

While P2P software is “free” to download, it comes at a high and undisclosed price to consumers. Consumers “pay” dearly for their use of this product through increased security vulnerabilities, reduced performance of their computers and lost privacy. They also subject themselves to a variety of legal risks, including prosecution for copyright infringement or even unlawful distribution of pornography. Teenagers and even children are among the most frequent users of P2P networks, and parents may not be aware their children have downloaded the software, or of the types of materials to which their children are thus exposed. This paper examines the undisclosed price (*i.e.*, injury) consumers incur in the use of P2P software, the role P2P providers play in causing that injury, and finally whether the P2P providers’ business practices violate Section 5 of the FTC Act or the Children’s Online Privacy Protection Act.

P2P software providers do not adequately, if at all, inform consumers of the security and privacy risks associated with downloading and using their software to share files over P2P networks. Specifically, these providers omit material information concerning the risk of viruses

¹ This paper was prepared on behalf of the Recording Industry Association of America.

that are spread throughout these networks. Nor do these providers adequately disclose that the software they offer comes bundled with third-party software that collects personally identifiable information from consumers. In some instances, this software monitors the unsuspecting user's key strokes and Internet sites visited. The disclosures P2P providers do provide of such matters, if any, often are buried in the fine print of lengthy End User License Agreements ("EULAs"). Consumers, including teens and children, who download P2P software from these sites most often do not understand these EULAs, assuming they even ever read them given their daunting length and complexity. Moreover, users may have no incentive to search for these buried disclosures in EULAs after reading some P2P providers' large print claims prominently displayed on their websites, which promise, for example, that the software contains no spyware, and otherwise highlight the benefits of the product without mentioning the very real risks associated with downloading files on P2P networks.

As a result of these deceptive practices, consumers are deceived regarding the ultimate amount of privacy and security risk involved with sharing files on P2P networks. Consequently, consumers suffer injuries in the form of viruses, widespread dissemination of their personally identifiable information, the clogging-up of their computer bandwidth and processing capacities, reams of spam e-mail, and, at the extreme, the unknowing and nonconsensual use of their computers by third parties. These deceptive and unfair acts, and the injuries they cause, warrant FTC investigation and possible enforcement action under Section 5. Such action would be consistent with past FTC enforcement actions against Microsoft, Guess, and others, for making deceptive promises to consumers about the safety of their personal information on the Internet.

An additional cost to P2P users is the litigation risk they face from using P2P software to engaged in unauthorized file sharing over the Internet. File-sharers, including many college students, are faced with the very real possibility of prosecution for such activities, as evidenced by the nearly 2,000 lawsuits filed since July of 2003 by the Recording Industry Association of America ("RIAA") on behalf of major record companies. The P2P providers do not adequately

warn their customers of this litigation risk, although some providers' EULAs include fine print disclaimers about how they do not condone copyright infringement. Some providers, such as Blubster, have gone even further and now advertise new P2P software that supposedly ensures users' anonymity so as to insulate the user from litigation risk.²

These representations raise several critical questions under Section 5. Do the P2P providers' assertions that they do not condone copyright infringement mislead users, particularly youthful, vulnerable users, into believing that file sharing on P2P networks is safe, when in fact just the opposite is true? Do P2P providers have the requisite substantiation under Section 5 to support such express and implied claims that, for example, use of certain software will protect users from being sued?

Finally, P2P networks raise a host of issues associated with the distribution of violent, pornographic and even illegal content. While the use of proper notice and labeling of violent or sexually explicit lyrics and other content has become a widespread practice among legitimate distributors of music and other media, such protections are nonexistent on P2P networks. Moreover, P2P software converts each in-network computer into a potential distribution channel for pornography, including illegal pornography. Such issues raise a myriad of issues under Section 5, including whether P2P providers should be required to disclose on their websites the risks associated with downloading violent, mature, pornographic or even illegal content, especially as these risks relate to the use of P2P networks by children.

An FTC investigation of P2P providers to further develop the facts and evidence related to the above consumer injuries attributable to the use of P2P networks, and enforcement actions if warranted, would advance consumer sovereignty – the core principle underlying consumer protection enforcement under Section 5. Such actions would assist consumers in making adequately informed decisions about the risks inherent in downloading and using P2P software.

² See Section V, *infra*.

II. THE RISE AND MECHANICS OF P2P FILE-SHARING

A. P2P File-Sharing Continues to Escalate

A multitude of Internet sites currently offer free downloads of P2P software. The identities of these sites are fluid and many new sites continue to emerge. During the first half of 2003 alone, “no fewer than 50 new versions of ‘peer-to-peer,’ or P2P file-trading software programs emerged on the Internet.”³ At the start of July 2003, the single most popular network, KaZaA, had a monthly audience in the U.S. of approximately 14 million unique users.⁴ The most popular sites, based on the total number of downloads of client software, are the following:

Software	Estimated Total Downloads ⁵
KaZaA Media Desktop 2.6	343 million
Morpheus 4.0.2	122 million
iMesh 4.2	71 million
Audiogalaxy Satellite 0.609	31.5 million
LimeWire 3.8.9	20.5 million
BearShare 4.4	19 million
Grokster 2.6	9 million
Blubster 2.5	4.5 million
Ares Galaxy 1.8.1	3 million
XoloX Ultra	2.5 million

³ Brian Krebs, *Online Piracy Spurs High-Tech Arms Race*, TechNews.com (June 26, 2003).

⁴ See Leslie Walker, *Music Pirates*, Post-Newsweek Business Information Inc. (July 20, 2003). “Unique Users” are defined as the total number of individuals who used the application in question at least once in the reported month. All unique users are unduplicated (only counted once). See Comscore.com Press Release, “Online Music Sales Decline Three Times Faster Than Overall Music Shipments, As File Sharing Applications Continue to Thrive” (Nov. 4, 2002).

⁵ Approximate number of total downloads of client software worldwide as of April 12, 2004. See www.download.com.

B. Mechanics of P2P File-Sharing

Consumers' downloading of music begins with a visit to an Internet website offering P2P client software, where consumers download P2P software and install it on their own computers free of charge or for a fee if they prefer "ad free" software. This process can take as little as a matter of minutes, depending on the speed of a user's Internet connection. Once installed on a user's hard drive, the software most often contains default settings that automatically make *all* files on each user's hard-drive – including but not limited to MP3 music files⁶ – available to the entire P2P network with no affirmative designation required by the user.⁷ The software enables each user to search, browse and download all files on the computers of other network users that have been automatically designated for "sharing," or in more limited instances, voluntarily designated.

As the chart above demonstrates, the major P2P networks include millions of users. Today's networks operate on a decentralized model, meaning that browsing and downloading of files occurs directly between network users (called "peers"), with no intervention by or reliance on a central host or server (the "peer-to-peer" model thus contrasts with a traditional "client-server" system used, for example, in most workplace network environments).

Music is by far the most popular type of file transferred on P2P networks. The ability to compress music into an MP3 format which is quickly and easily transferred with no discernable loss in sound quality has contributed significantly to the growth of file sharing on P2P networks.⁸

⁶ MP3 is currently the most widely used digital format for music. Developed in the 1980s, the MP3 format is based on an algorithm that compresses a digital music file so that it can more easily and quickly be copied and transferred over the Internet.

⁷ Pew Internet & American Life Project, *Music Downloading, File-Sharing and Copyright* (July 2003); see FTC Consumer Alert, *File Sharing: A Fair Share? Maybe Not* (July 2003) ("If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but all other information on your hard drive.").

⁸ Another factor facilitating the growth of file sharing has been the steady increase in capacity of most commercially available computer hard-drives. In 1992, the average PC hard-drive was 120 megabytes. Today, the average hard-drive has a capacity of 40 gigabytes, more than a 300 times greater increase. Les Grossman, *It's All Free*, Time (May 5, 2003). This enables a user to store many more digital files (including MP3 files) on his or her computer.

Once logged onto a P2P network, a user can conduct a simple keyword search for a desired artist and/or title, or opt simply to browse through the files made available by other users.

Files stored on computers with broadband Internet connections remain available for sharing on the network regardless of whether the individual user is using the computer or has an Internet browser open at the time. “If you have a high-speed or ‘broadband’ connection to the Internet, you stay connected to the Internet unless you turn off your computer or disconnect your Internet service. These ‘always on’ connections may allow others to copy your shared files at any time. What’s more, some file-sharing programs automatically open every time you turn on your computer.”⁹

III. PROVIDERS OF P2P SOFTWARE DO NOT ADEQUATELY DISCLOSE THE RISK OF VIRUSES ON P2P NETWORKS

The FTC and others have noted that the spread of viruses over P2P networks is a common, material danger associated with P2P usage. As the FTC warned consumers in July 2003, “[f]iles you download could be mislabeled, hiding a virus or other unwanted content.”¹⁰ The FTC’s warning is supported by substantial evidence which demonstrates that P2P networks are a virtual grid through which viruses are broadly disseminated among consumers. Internet sites that distribute P2P file-sharing software, however, contain no clear and conspicuous warnings or disclosures about the risks associated with downloading a virus through file sharing on P2P networks.

There is a high risk that P2P network users’ computers will be infected with a virus. These viruses are commonly distributed throughout the Internet in general, while others are specifically designed for dissemination through P2P networks. Our initial analysis, based on information provided by Symantec Security and attached as **Exhibit 1**, shows that many of the most dangerous computer viruses in existence are spread on the major P2P networks. Over one

⁹ FTC Consumer Alert, *File Sharing: A Fair Share? Maybe Not* (July 2003).

¹⁰ *Id.*

hundred of these viruses are found on KaZaA and Morpheus. A significant number of viruses also appear on Limewire, iMesh, BearShare, and Grokster. These viruses often are masked as seemingly desirable files that consumers, particularly children, would want to download. As shown on **Exhibit 2**, these viruses appear on P2P networks under file names such as “The Ermine Show (Full Album).exe,” and “Lord of the Rings Screensavers.scr.” Utilizing file names associated with these and other pop culture icons, viruses traded on P2P networks often are capable of avoiding anti-virus software installed on a user’s computer or a corporation’s network, as the requesting user has voluntarily requested to receive the file, not knowing it is infected. Thus, viruses traded on P2P networks “can circumvent most email or Web download anti-virus solutions.”¹¹

The viruses impose grievous harm for individual consumers misfortunate enough to download them. For example, W32.HLLW.Maax@mm is a virus that spreads through Microsoft Outlook and several P2P software programs. The virus specifically targets users of KaZaA, Morpheus, Edonkey, Grokster, Limewire, and BearShare, although it can be spread through other programs as well. System files from the P2P programs are overwritten by the virus name, introducing the virus onto the host computer. After this has been completed, the virus modifies the Autoexec.bat file. The next time the computer is restarted, the modification will automatically cause the C and D drives to be formatted. The virus will also attempt to halt any anti-virus or security processes that attempt to shut it down.¹²

Another virus, W32.Naco.D@mm, of which there are many variants, operates in a similar manner. In this case, however, the author of the virus has compressed and encrypted the virus so that any attempts to remove it by antiviral software will be delayed. The virus searches for specific folders, many of which are specific to P2P programs such as KaZaA, Morpheus,

¹¹ Palisade Systems, Executive Summary of Peer-to-Peer Study Results at 3 (March 2003).

¹² Symantec Security Response – W32.HLLW.Maax@mm, <http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.hllw.maax@mm.html>.

Limewire, Grokster, and BearShare. If these folders are found on the system, the worm copies itself into the folder using a variety of names. All other files in the same folder as the viruses are deleted, and the D drive is completely formatted. By using various pseudonyms, the virus can run many copies of itself at the same time, disrupting the host system further and making anti-virus attempts more difficult.¹³

Another example is Fizzer, a virus that plagued KaZaA users in May 2003:

KaZaA and KaZaA users' susceptibility to viruses is well illustrated by the Fizzer worm discovered in May 2003. Fizzer spreads through the KaZaA network by creating multiple copies of itself with different names and placing them in the victim computer's dedicated KaZaA file-sharing folder. As soon as this happens, Fizzer becomes "available" to every other KaZaA user.

Fizzer is a dangerous worm. It includes a keylogger that intercepts and records all keyboard strokes into a separate log file, and a backdoor utility that allows the worm's "master" to control the infected computer via IRC (Internet Relay Chat) channels as well as via HTTP and Telnet protocols. It also attempts to download updated versions of its own executable modules, and scans the memory of victim computers to shut down the active processes of a range of the most widely used anti-virus programs.¹⁴

Viruses like Fizzer can devastate an individual user's computer, making it virtually unusable and beyond repair. Moreover, through e-mails, an unknowingly infected P2P user may spread the virus to others not sharing files on a P2P network. Such dangers are especially ripe for business computer networks, where infected files downloaded by one employee can spread rapidly throughout the network via inter-office e-mail.

Despite these known and real dangers, the providers of P2P software provide little to no disclosure of the risks to consumers. Indeed, a preliminary review of the Internet sites of major

¹³ *Symantec Security Response* – W32.Naco.D@mm, <http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.naco.d@mm.html>.

¹⁴ *KaZaA: The Hidden Threat from Peer-to-Peer Networks*, PestPatrol Educational White Paper at 7 (June 2, 2003).

P2P software providers revealed *no* clear and conspicuous disclosures on the risks of contracting a computer virus via file sharing on P2P networks.¹⁵ This complete lack of disclosure by P2P providers warrants an FTC investigation as to whether P2P providers are violating Section 5 by failing to include material information regarding the risks of viruses inherent in their software programs.

IV. CONSUMERS ARE HARMED THROUGH P2P SOFTWARE PROVIDERS' POTENTIALLY DECEPTIVE PRACTICES CONCERNING SPYWARE/ADWARE

Another consumer harm associated with the acquisition of P2P software arises from the unknowing acquisition of spyware/adware. A consumer may acquire this software either through downloading P2P software from providers such as KaZaA, Morpheus and Limewire, or through the files the consumer subsequently downloads off P2P networks.¹⁶

P2P software providers often partner with the providers of adware/spyware, profiting on the inclusion of such third-party software with their popular P2P programs. The fundamental purpose of spyware is “to gather information about the user and relay it back to the ad server so

¹⁵ The largest P2P software provider, KaZaA, while not clearly and conspicuously disclosing the risk of viruses on P2P networks, evidently is aware that such risk exists. Specifically, among the embedded software that downloads automatically with the KaZaA software is Bullguard P2P, software designed to guard users' computers from virus attacks on P2P networks. This discussion of Bullguard is buried on page 5, paragraph 9.4.3 of KaZaA's EULA. While KaZaA should be, perhaps, applauded for taking steps to safeguard its users' computers against viruses spread through P2P networks (although we currently have no data on the actual effectiveness of this software at preventing viruses), this still does not remedy KaZaA's lack of clear and conspicuous disclosure to consumers of the risks associated with virus attack on P2P networks before they download or purchase KaZaA's software. *See Federal Trade Commission Policy Statement on Deception, appended to Cliffdale Assocs.*, 103 F.T.C. at 180 (Disclosures of qualifying information must be clear and conspicuous. Moreover written disclosures or fine print may be insufficient to correct a misleading representation – in this case, that KaZaA's software is safe to use.) (hereinafter “Deception Statement”). Moreover, as explained above, many of the viruses spread through the P2P networks are immune to the antiviral software.

¹⁶ *See* Center for Democracy & Technology, Comments and Request to Participate: FTC April 2004 Spyware Workshop at 2 (March 5, 2004) (“‘Spyware’ . . . maybe bundled with other free applications, including peer-to-peer file sharing applications [or] may be distributed through deceptive downloading practices.”) (hereinafter “CDT Comments”); Palisade Systems, Executive Summary of Peer-to-Peer Study Results at 2 (March 2003) (“Applications such as KaZaA and BearShare require users to install spyware on their computer as part of the licensing agreement. Spyware tracks the activities of the user and reports them to a third-party organization.”).

that accurately targeted advertising can be directed at the user.”¹⁷ Such transmission of information most often occurs without the user’s knowledge. Spyware also can hijack a consumer’s computer, making its contents and storage capacity available to others without a consumer’s knowledge or consent. Other problems, such as using up computer bandwidth and processing capacity, and dramatically increasing spam, also are attributable directly to spyware/adware.

A recent study by the University of Washington finds that P2P networks play a central role in the dissemination of spyware. Researchers downloaded the ten most popular shareware/freeware programs, as listed in CNet’s download.com website. Of the four programs containing spyware, three (KaZaA, iMesh and Morpheus) were P2P file sharing clients. “Assuming CNet’s data is correct,” the study concludes, “hundreds of millions of users have been exposed to spyware from this source alone.”¹⁸

While the computers of all Internet users can become infected with spyware, this study found that users of P2P software are much more likely to acquire spyware than Internet users in general. Specifically, users of KaZaA’s P2P software were up to *22 times* more likely to become infected with spyware than Internet users in general, “confirming the intuition that using file-sharing software exposes clients to spyware.”¹⁹ As the study concludes, consumers who acquire spyware on their computers face multiple serious risks.

Spyware poses several risks. The most conspicuous is compromising a user’s privacy by transmitting information about that user’s behavior. However, spyware can also detract from the usability and stability of a user’s computing environment, and has the potential to introduce new security vulnerabilities to the

¹⁷ *Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security*, PestPatrol Technical White Paper (April 2, 2003).

¹⁸ Stefan Saroiu, Steven D. Gribble and Henry M. Levy, “Measurement and Analysis of Spyware in a University Environment,” (<http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf>) at 2 (hereinafter “Saroiu”).

¹⁹ Saroiu at 9.

infected host. Because spyware is widespread, such vulnerabilities would put millions of computers at risk.²⁰

A. P2P Software Providers Fail to Adequately Disclose to Consumers the Inclusion of Spyware/Adware

Many major providers of P2P software claim to be spyware-free. For example, Limewire states prominently on the opening page of its Website that its software contains “[n]o spyware . . . EVER!”²¹ A third-party source quotes Sharman Networks, the distributor of KaZaA, as claiming that “KaZaA Media Desktop (KMD) . . . made available on KaZaA.com or Download.com . . . contains **NO** spyware. Sharman Networks does not condone the use of spyware nor support the distribution of spyware to others.”²² P2P software provider Morpheus claims that it “does not bundle malicious spyware.”²³

A preliminary review of the software provided by KaZaA, Limewire, Morpheus and other P2P providers indicates, however, that such claims are likely deceptive or outright false because 1) the providers fail to clearly and conspicuously disclose that various third-party software products come imbedded in the P2P software they provide; and 2) as detailed below, the claims may not be substantiated. Whether this third-party software is called “adware” (as preferred by the P2P providers) or “spyware” (as used by others) is irrelevant. What is relevant under Section 5 is that such software is included with the P2P software consumers download, most often without knowledge or consent, and after downloading this software collects and transmits personally identifiable consumer information to third parties, as well as causes other consumer injuries.²⁴

²⁰ *Id.*

²¹ www.limewire.com

²² *KaZaA: The Hidden Threat from Peer-to-Peer Networks*, PestPatrol Educational White Paper (June 2, 2003).

²³ www.morpheus.com/notices.html

²⁴ *See* Saroiu at 1 (“[T]he term ‘spyware’ is commonly used to refer to software that, from a user’s perspective, gathers information about a computer’s use and relays that information back to third party. This data collection occurs sometimes with, but often without, the knowing consent of the user.”).

While P2P software providers fail to tell consumers the whole story when it comes to bundled third party software, others that distribute their products are much more cautious. For example, contrary to Limewire's claim on its own website that no spyware, ever, is included with its software, a third-party distributor of this software tells a different story, warning its own customers that Limewire's software "includes additional applications bundled with the software's installer file. Third-party applications bundled with this download may **record your surfing habits, deliver advertising, collect private information, or modify your system settings.**"²⁵

Similarly, contrary to claims by Morpheus that it does not bundle "malicious spyware" with its P2P software, the University of Washington study found the opposite, that versions of Morpheus' P2P software contained spyware.²⁶ This study also found a specific type of spyware, eZula, bundled with Limewire (contrary to its "[n]o spyware . . . EVER!" representation).²⁷

KaZaA, by far the most popular P2P software, has been a principal distributor of spyware since its initial release early this decade. As shown on the following chart, twelve different spyware/adware programs have been bundled with its software, and *every* version of KaZaA's P2P software released this decade has had at least two versions of spyware bundled with it. *Like many P2P programs, users cannot acquire KaZaA's P2P software without also acquiring the third party software bundled with it.*

²⁵ www.download.com (emphasis in original).

²⁶ See Saroiu at 3.

²⁷ See *id.* at 5.

Spyware Bundled with KaZaA P2P Software									
KaZaA Version	1.3.3	1.4	1.5	1.6	1.7	2.0	2.1	2.1.1	2.6
Released	12/01	01/02	02/02	04/02	05/02	09/02	02/03	05/03	11/03
Gator									X
SaveNow	X	X	X	X	X	X	X	X	X
Cydoor	X	X	X	X	X	X			
BDE	X	X	X	X	X	X			
VX2	X	X							
New.net	X	X	X	X	X	X			
OnFlow	X	X						X	
D/L-Ware					X	X	X		
CmnName	X	X	X	X	X	X			X
PromulGate						X			
DirectTVIcon			X	X					
MySearch									X

Source: Saroiu at 4.

If P2P providers do make disclosures about the spyware/adware incorporated with their products, such disclosures are buried in the fine print of EULA agreements. For example, on page six of its nine-page EULA, P2P provider Grokster discloses that its software may be bundled with spyware/adware and that the consumer should “note that the THIRD PARTY SOFTWARE is subject to different license agreements or other arrangements, which should be read carefully, compared to the Terms of Service of Grokster.”²⁸ While failing to provide a comprehensive list of all adware/spyware bundled with Grokster, making it virtually impossible to conduct the due diligence Grokster pawns off on its customers, the Grokster EULA goes on to provide three paragraphs noting the “inherent dangers” of using third party software downloaded from the Internet, and disclaiming all liability. Similarly, P2P provider iMesh urges its customers to review carefully the license agreements of its third party software providers (without disclosing the identity of these providers) and disclaims all liability for third party software – in Section 9 of its multi-page, small font EULA.

Even if P2P sites like Grokster and iMesh provide their customers notice regarding the due diligence they suggest their users conduct, it is doubtful that reasonable consumers of P2P software, many of whom are teenagers and children, 1) can find and understand the disclosures;

²⁸ Grokster EULA at 6.

and 2) can or do actually conduct the due diligence the P2P providers conveniently lob to the user. This failure to adequately disclose is particularly egregious given that: “Many of the most popular file sharing applications do come bundled with spyware. . . . Peer-to-peer applications are some of the worst culprits when it comes to obscuring notice by bundling EULAs together and making uninstallation of spyware components as difficult as possible.”²⁹

B. Spyware Distributed With P2P Software Compromises Consumer Privacy

Most users, if not all, are unaware of the information-gathering functionality of spyware programs. Spyware is generally freeware, and the information-gathering functionality is not mentioned before users install the software.³⁰

The deceptive bundling of adware/spyware with P2P software results in many forms of consumer injury, including a severe compromise of consumer privacy. For example, despite their “no spyware” pledges, an embedded software included in KaZaA and Limewire (as well as other P2P providers like iMesh and Grokster) is Cydoor.³¹ Cydoor is one of the most widely spread versions of spyware.³² It “delivers highly targeted advertising directly to desktops in advertising enabled software applications.”³³ The targeted advertisements that Cydoor delivers are dictated by information it collects on individual user’s demographics and Internet browsing history.³⁴ “When a user first installs a program that contains Cydoor, the user is prompted to fill out a demographic questionnaire, the contents of which is transmitted to the

²⁹ *Ghosts in Our Machines: Background and Policy Proposals on the “Spyware” Problem*, Center for Democracy & Technology White Paper at 10 (Nov. 2002) (hereinafter “CDT White Paper”).

³⁰ *The Dangers of Spyware*, Symantec Security White Paper (2003).

³¹ *See, e.g.*, KaZaA EULA ¶ 9.4.1.

³² *See* Saroiu at 4.

³³ www.cydoor.com

³⁴ *See* Saroiu at 4.

Cydoor servers.”³⁵ Thereafter, “Cydoor collects information about certain Web sites that a user visits and periodically uploads this data to its central servers.”³⁶ In addition to collecting such personal information without consent, there also have been “[n]umerous reports of Cydoor and associated applications causing errors in Windows XP.”³⁷

Despite these harms, consumers who desire KaZaA must also acquire Cydoor, often unknowingly. “*In Kazaa there is at least one program, Cydoor, that you cannot opt out of, and if you remove that, Kazaa stops working until you reinstall it.*”³⁸

Another third-party software distributed with KaZaA, iMesh, Grokster, and other P2P providers is the GAIN Adserver software, also known as Gator, which “identifies your interests based on . . . your computer usage and uses that information to deliver advertising messages to you.”³⁹ Gator has been one of the most rapidly expanding examples of spyware/adware, and “has been among the most frequently cited pieces of privacy-invading spyware.”⁴⁰ To provide targeted advertising, Gator’s software “can track users’ web-browsing, including gathering and transmitting information on search terms.”⁴¹ Versions of Gator also have been known to keep track of a user’s location, zip code, and computer ID, and have been found to remain on a user’s computer long after the P2P software was removed.⁴²

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

³⁸ Lisa Gill, *PC Spies at the Gate*, NewsFactor Network (Jan. 2, 2003) (emphasis added).

³⁹ *See, e.g.*, KaZaA EULA ¶ 9.4.4.

⁴⁰ CDT White Paper at 4 n.3. The University of Washington study found that the prevalence of Gator throughout computers on the university’s network had increased nearly 600% from 2000 to 2003. *See Saroiu* at 7.

⁴¹ CDT White Paper at 4 n.3.

⁴² *See id.*; *accord Saroiu* at 4.

Cydoor and GAIN/Gator are just two examples of software, included in downloads of P2P software, which transmits personally identifiable information to third parties without a consumer's knowledge or consent. Further investigation of P2P providers by the FTC likely would reveal other examples.⁴³ Indeed, there are hundreds if not thousands of consumer complaints regarding the injury suffered as a result. A quick search on a single public website generated 687 consumer complaints on KaZaA's software alone. A few excerpts demonstrate the harms inflicted on these consumers. *See Exhibit 3.*⁴⁴

“Crashed my computer!!! Virus infected 54 files on my hard drive. I had to download another adware killer to get rid of all the adware. If you do download, you need to get Spyware S&D to kill the adware after you take Kazaa off . . . and you will take it off.”

“Kazaa now has pop up ads that leave the Trojan virus JS/noclose on your computer so you can't close the ads. It happens at least every hour. There is no way to contact them about this problem either. DO NOT DOWNLOAD!!!”

“I never had any problems with Password stealing viruses until I downloaded this junk program and most viruses were directly linked to the advertising popups and other adware junk bundled with this very Slow loading program. Make sure you have a Very Good antivirus program that is on at all times if you use this file sharing program, you'll need it a lot.”

“I had this on my computer for less than 2 weeks and during that time I got a virus that was not cleanable because it damaged so many files. I finally had to restore my computer after many hours of tech support and virus scanners that could not fix it. I would never recommend this to ANYONE!!!”

⁴³ See *Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security*, PestPatrol Technical White Paper (April 2, 2003) (listing twelve embedded software products included with Grokster's P2P software).

⁴⁴ The complaints were made by users of KaZaA software specifically regarding the burden of viruses that can be spread by the use of KaZaA and other P2P software programs. These and other complaints can be found on-line at http://download.com/3302-2166_4-10247401.html?pn=1&fb=2.

C. There are a Myriad of Additional Consumer Harms Caused by Adware/Spyware

In addition to seriously compromising consumer privacy and crashing consumers' computers via viruses, spyware/adware cause additional harms to the computers of consumers or, for consumers who download P2P software at their work, to computer networks of both large and small businesses. The transmission of personal information from, and targeted advertisements to, a user's computer from spyware/adware can appropriate much of a computer's or network's broadband capacity. Such constantly running software also can use substantial portions of a computer's or network's processing capacity. Since P2P software often includes more than one embedded spyware program, the simultaneous running of such software can multiply these effects.⁴⁵ These cumulative effects are magnified on corporate computer networks, with multiple versions of P2P software installed on multiple employees' computers.

The targeted advertisements spyware/adware are designed to create also increases the amount of spam e-mail distributed throughout the Internet. "Spyware will often locate email addresses and phone numbers with them. These addresses then get added to other addresses and passed between spammers."⁴⁶ As the FTC is well aware, the rise of spam e-mail has become a major burden on consumers and the American economy, collectively costing businesses in the U.S. an estimated \$8.9 billion.⁴⁷ Moreover, the rise of spam has diminished significantly the value of the Internet to consumers.

Additionally, certain forms of spyware hijack a user's computer and Internet connection and use it for their own purposes. A prominent example of this was the distribution of the Altnet software through KaZaA in April 2002.⁴⁸ The goal of Altnet was to create a storage and

⁴⁵ See *Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security*, PestPatrol Technical White Paper (April 2, 2003).

⁴⁶ *Id.*

⁴⁷ *See id.*

⁴⁸ *See* CDT White Paper at 4.

computing network grafted upon the KaZaA P2P network, from which its creator, Brilliant Digital Entertainment, could sell spare computing capacity located on users' computers to third parties. Despite this intended third-party use of a consumer's computer, "[u]sers were never clearly told that software with the capability to use their computers and network connections in this way was being installed."⁴⁹

Finally, in addition to being hard to detect, many spyware programs are difficult to delete, and may remain active even after a consumer deletes the associated P2P program. "[O]nce these invasive applications are on a user's computer, they can be difficult or impossible to find and remove."⁵⁰ This viability is due in part to spyware's ability in many instances "to *self-update*, or download new versions of themselves automatically. Self-updating allows spyware authors to introduce new functions over time, but it also may be used to evade anti-spyware tools, by avoiding specific signatures contained within the tools' signature databases."⁵¹

V. P2P PROVIDERS FAIL TO ADEQUATELY WARN USERS OF LITIGATION RISKS

It is an established fact that many users download their file-sharing software for the purpose of exchanging copyrighted materials. In fact, some P2P providers appear to implicitly endorse and explicitly facilitate such use. For example, Grokster's software extracts "meta data" from imported files, and then arranges the meta data so that it is searchable by other users.⁵² For music files the meta data extracted by the Grokster program "comprises Title, Album, Artist, Length, and bit rate."⁵³ Grokster suggests that extracting and organizing the meta data increases the search possibilities and accuracy of its file-sharing software. However, to use such meta data

⁴⁹ *Id.*

⁵⁰ CDT Comments at 3.

⁵¹ Saroiu at 3.

⁵² See Grokster "Technology" Web Page, accessible at www.grokster.com.

⁵³ *Id.*

for searching, users must know the title, album, etc., information that presumably users are not likely to know for most uncopyrighted works.

At least two P2P providers acknowledge in their EULAs that they are aware of the use of their software to exchange materials without the knowledge and consent of the copyright owners.⁵⁴ However, it is the consumer user, often college students and younger, who suffers the harm. The RIAA, on behalf of major record companies, has brought close to 2,000 lawsuits since July of 2003 against individual users of P2P networks, including bringing in March 2004 actions against 532 students at 21 different universities.⁵⁵ While P2P providers' do make some disclaimers regarding the litigation risk their users face, these disclosures are often buried in the depths of fine-print EULAs.⁵⁶ Consumer perception evidence likely would demonstrate that these disclaimers are inadequate to warn consumers about the litigation risk inherent in downloading music on P2P networks. Moreover, even if users find and read the P2P's fine-print disclosures,⁵⁷ the statements may imply to the user that the P2P providers are actively policing their networks, when just the opposite is true.

Some providers have actually developed new software versions designed to circumvent detection of the identity of P2P network users. A recent Blubster press release proclaims "Blubster has re-launched with a new, secure, decentralized, self-assembling network that

⁵⁴ See, e.g., Grokster Terms of Service ¶ 7 ("You should be aware that some of the files other Grokster users designate to share may have been created or distributed without the copyright owners' authorization."); Audiogalaxy "Disclaimer and Usage Agreement" ("Audiogalaxy cautions you that some music on the Internet has been made available against the wishes of the copyright owners.").

⁵⁵ See RIAA Press Release, "RIAA Brings New Round of Cases Against Illegal File Sharers" (March 23, 2004).

⁵⁶ See, e.g., KaZaA EULA ¶ 6.1; Grokster EULA ¶ 1; Audiogalaxy Disclaimer and Usage Agreement ¶ 1.

⁵⁷ See, e.g., www.Morpheus.com/notices.html "Copyrights and Inventions," ("StreamCast [Morpheus] does not condone copyright, patent, or other intellectual property infringement."); www.Audiogalaxy.com/info/help ("Audiogalaxy respects the intellectual property of others, and we ask our users to do the same. Audiogalaxy may, at its own discretion, disable the accounts of users who may be infringing the intellectual property of others."); Grokster EULA ¶ 1 ("Please note that Grokster respects the right of copyright owners and is fully committed to protect their rights.").

provides users with anonymous accounts.”⁵⁸ The new version, “takes advantage of a new streamlined means of distributing large files to disassociate file transfers from specific users.”⁵⁹ Blubster goes on to state, however, in small-print, at the very bottom of its press release separate and distinct from the rest of its text, that “Blubster.com does not condone activities and actions that breach copyright owners, and it is user’s responsibility to obey all laws governing copyright in each country.”⁶⁰ This is precisely the kind of inadequate disclosure the FTC uses as Example 3 in the guidance on Dot Com Disclosures, which states that blank space between on-line claims and their required disclosures fails to make the disclosures clear and conspicuous as required under Section 5. Compare **Exhibit 4** to **Exhibit 5**. Indeed, Blubster’s press release is even worse than the FTC example, given the small font size of the disclosure’s text.

These P2P provider practices raise significant Section 5 questions such as whether the P2P providers have clearly and conspicuously disclosed to users the risks of sharing files on P2P networks. In addition, do the providers’ fine-print EULA disclosures concerning unauthorized file sharing mislead users into believing that there is minimal risk of downloading copyrighted materials because the providers affirmatively police the P2P networks for such materials? Do providers’ claims of software to mask users’ identity mislead consumers into believing they are safe from being sued? Finally, do P2P providers have the requisite substantiation to support claims that their software allegedly insulates users from this litigation risk?

⁵⁸ Blubster Press Release, “P2P Downloaders Go Anonymous with Blubster 2.5” (June 30, 2003).

⁵⁹ *Id.*

⁶⁰ *Id.*

VI. PROVIDERS FAIL TO WARN USERS OF VIOLENT OR OFFENSIVE MATERIALS AVAILABLE THROUGH THEIR NETWORKS AND OF THE RISK OF USERS BECOMING UNWITTING DISTRIBUTORS

As discussed below, many P2P users are teenagers (and even younger children),⁶¹ whose parents may wish to limit access to lewd, violent or offensive materials. The FTC has recognized this parental interest in a series of reports on marketing of violent entertainment to children, and has sought to encourage media distributors to adopt practices that empower parents to make informed decisions about their children's exposure to such materials, including appropriate notices and labeling in advertising and packaging.⁶² The Commission has noted that the music recording industry has made progress in these respects,⁶³ and the RIAA has indicated its commitment to continue working with the Commission to achieve still further improvement.

Even as legitimate music distributors are making progress towards empowering parents, P2P services continue to offer an environment where – literally – anything goes. Indeed, children of any age may download P2P software and, having done so, access unlabeled music, images and video files of virtually any kind. Children need not even act willfully to access inappropriate material: It is easy to imagine a teenager downloading a file named “Britney Spears.mpeg” expecting to find a song by Ms. Spears -- and receiving instead content her parents would find highly inappropriate. P2P services not only fail to provide for the type of labeling now universally adopted by legitimate distributors; they make no significant effort of any kind to

⁶¹ See *infra* Section VII.C (citing data which show that as many as 8.7 million Americans between the ages of 12 and 17 engage in file sharing on P2P networks).

⁶² See FTC Report, “Marketing Violent Entertainment to Children: A Twenty-One Month Follow-Up Review of Industry Practices in the Motion Picture, Music Recording and Electronic Game Industries – Report to Congress” (June 2002); see also FTC Report, “Marketing Violent Entertainment to Children: A Review of Self-Regulation and Industry Practices in the Motion Picture, Music Recording and Electronic Game Industries,” (Sept. 11, 2000); Letter from former FTC Chairman Robert Pitofsky to Senator John McCain, Chairman, Committee on Commerce, Science, and Transportation regarding the FTC Report on Marketing Violent Entertainment to Children (Nov. 20, 2000) (“[T]he Commission believes that the best course is for the Congress to continue efforts to promote substantially improved, voluntary, self-regulatory [industry] efforts [to label violent movies, music or electronic games regarding their appropriateness for children].”).

⁶³ See Marketing Violent Entertainment to Children, *supra* note 62 at 18.

notify parents of the types of materials their children will find when they start “sharing” files with anonymous fellow P2P subscribers of all ages and tastes. To the extent such warnings, if available, would influence the decisions of parents on whether to allow their children to utilize P2P services, their absence may constitute a material omission subject to scrutiny under Section 5.

Another issue that raises questions of the need for warning disclosures is pornography, especially illegal pornography, shared over the P2P networks. Most file-sharing software configures itself so that any file that a user downloads becomes available for redistribution from that user’s computer *to anyone else using the P2P network*. Thus, *file-sharers who download files for private, home use become distributors* of those files by (perhaps unwittingly) turning their home computer into a public content-distribution source. This can result in exposing children to pornography and adults to criminal liability for illegal pornography distribution. The question under Section 5 is again whether P2P providers failure to warn users of the risk of prosecution for pornography distribution (albeit unintended) constitutes an unfair or deceptive practice, particularly when many of the P2P users are teenagers or children.

VII. AN FTC INVESTIGATION IS WARRANTED TO DETERMINE WHETHER P2P PROVIDERS’ BUSINESS PRACTICES VIOLATE THE FTC ACT

The acts and practices of the P2P providers raise significant questions as to whether violations of Section 5 of the FTC Act have occurred. Section 5 prohibits unfair or deceptive acts or practices in or affecting commerce.⁶⁴ A representation, omission, or practice is deceptive if it is likely to mislead consumers acting reasonably under the circumstances to their detriment.⁶⁵ In determining the claims that an ad conveys to consumers, the FTC looks at the

⁶⁴ 15 U.S.C. § 45

⁶⁵ See, e.g., *Kraft, Inc.*, 114 F.T.C. 40, 120 (1991), *aff’d and enforced*, 970 F.2d 311 (7th Cir. 1992); *Cliffdale Assocs.*, 103 F.T.C. 110, 164-65 (1984); see generally Deception Statement at 174-83.

ad's "net impression."⁶⁶ When representations are targeted to a specific audience, including vulnerable groups such as children, the Commission considers the effect of the representation on a reasonable member of that vulnerable group.⁶⁷ Disclosures of qualifying information must be clear and conspicuous. Written disclosures or fine print may not be sufficient to correct a misleading representation.⁶⁸ Omissions constitute deception when 1) a seller states a "half-truth" or 2) the seller is silent "under circumstances that constitute an implied but false representation."⁶⁹

An act or practice is unfair if it causes or is likely to cause injury to consumers that is 1) substantial; 2) not outweighed by countervailing benefits to consumers or competition; and 3) not reasonably avoidable by consumers themselves.⁷⁰ In determining whether an act is unfair, the Commission may consider established public policy as evidence, but public policy considerations may not serve as the primary basis for an unfairness decision.

Application of the FTC's deception and unfairness standards evidences that an FTC investigation of P2P providers is warranted.

A. P2P Providers Have Engaged in Deceptive Representations and Failed to Disclose Material Facts

The above discussion indicates that P2P software distributors do not tell the consumers the whole story or even the highlights concerning the risks inherent in the software they distribute. Since the rise to prominence of the Internet in the late 1990s, the FTC has been

⁶⁶ *FTC v. Sterling Drug*, 317 F.2d 669, 674 (2d Cir. 1963).

⁶⁷ *See* Deception Statement at 179 (citing *Bates v. Arizona*, 433 U.S. 350, 383 n.37 (1977)).

⁶⁸ *See id.* at 180.

⁶⁹ *International Harvester Co.*, 104 F.T.C. 949, 1058 (1984); *see also* Deception Statement ("The representation, omission or practice must be a 'material' one. The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service.")

⁷⁰ *See* 15 U.S.C. § 45(n); *see also*, *Orkin Exterminating Co.*, 108 F.T.C. 263, 362 (1986); *International Harvester Co.*, 104 F.T.C. 949, 1061 (1984); *see generally* *Federal Trade Commission Policy Statement on Unfairness, appended to International Harvester Co.*, 104 F.T.C. at 1070-76.

at the forefront of protecting consumers' interests in the digital marketplace. Specifically, it has encouraged Web site operators to "provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it . . . how they use it . . . and whether other entities are collecting information through the site."⁷¹ Operators also should "take reasonable steps to protect the security of the information they collect from consumers."⁷² When Web site operators fail to deliver on their promises of safeguarding consumer information, the FTC has taken enforcement action.⁷³

An investigation and, if warranted, enforcement actions against P2P software providers is consistent with these principles. Indeed, the potentially unfair and deceptive practices described above, and the substantial consumer injuries they impose, appear to be even more egregious than those involved in arguably analogous FTC enforcement actions. For example, among other claims, the FTC alleged that Microsoft misrepresented the level of security for consumers using Microsoft's Passport authentication services to make purchases on the Internet, claiming that purchases made with Passport were more secure when, in fact, this was not true.⁷⁴ P2P software providers, however, misrepresent or fail to disclose the substantial risks consumers face by downloading and using their products. Thus, while Microsoft's Passport service did not provide the additional security benefits it promised, it did not, like P2P software, place a consumer at *greater* risk of harm without the consumer's knowledge or consent.

The FTC's actions against Eli Lilly and Guess involved these parties' negligence concerning the security of information provided by consumers. Specifically, Eli Lilly breached

⁷¹ Robert Pitofsky, *Prepared Statement of the Federal Trade Commission on "Privacy Online: Fair Information Practices in the Electronic Marketplace"* before the Senate Committee on Commerce, Science, and Transportation (May 25, 2000).

⁷² *Id.*

⁷³ See Orson Swindle, *Prepared Statement of the Federal Trade Commission on "Cybersecurity and Consumer Data: What's at Risk for the Consumer?"* before the Commerce, Trade & Consumer Subcommittee of the House Committee on Energy and Commerce (Nov. 19, 2003).

⁷⁴ See Microsoft Corp. File No. 012 3240, FTC Analysis to Aid Public Comment (2002).

its promise to keep customer information confidential by mistakenly disseminating a mass e-mail that contained its individual customers' e-mail addresses.⁷⁵ Guess did not satisfy its promises of confidentiality and security to consumers when it knew that its system was not secure and a hacker subsequently gained access to consumer information by using an SQL attack.⁷⁶

What P2P providers have in common with the Eli Lilly and Guess actions is the unconsented-to dissemination of confidential consumer information. However, in the case of P2P software distributors, this breach in consumer trust is not the result of negligent employee action (as in Eli Lilly) or the hacking into a system by a third party (as in Guess). The invasion of consumer privacy in this instance is caused by a consistent business practice knowingly followed by major P2P software providers – profitably partnering with third party software suppliers who acquire confidential consumer information and then failing to disclose or, alternatively, burying disclosure of the existence of such relationships deep within EULA fine-print.

Enforcement against providers of P2P software also would be consistent with older Commission precedent that prohibited the unauthorized sale of cable television decoder boxes to consumers. In its 1987 decision against C & D Electronics, the Commission concluded that the sale of decoder boxes, which enabled their purchasers to acquire cable television for free, hurt all consumers through harms like increased cable subscription rates and eventual reductions in cable services.⁷⁷

The RIAA has stated that unauthorized distribution through P2P networks reduces substantially the ability of the record industry to find and develop new talent.⁷⁸ Therefore, in the long term all music fans are injured through a reduction in the quantity and quality of new music

⁷⁵ See Eli Lilly and Co., FTC Complaint (May 2002).

⁷⁶ See Guess?, Inc., FTC Complaint (July 2003).

⁷⁷ See *In the matter of C&D Electronics, Inc.*, 109 F.T.C. 72 (1987).

⁷⁸ See www.riaa.com.

the industry is capable of providing. This form of an output reduction is similar to that Chairman Oliver described over fifteen years ago arising from the sale of cable decoder boxes:

[I]n a case of this sort injury to consumers may go well beyond a simple increase in prices; the activity here may provide disincentives that will result in services not being available to consumers at all. There is little or no reason for businesses to establish cable services, or to expand and improve existing ones, unless sufficient revenue can be generated to warrant expenditures. Widespread or unchecked free riding could discourage venturers that would offer such services or could result in raising the prices for cable subscriptions in existing networks beyond optimal levels. Thus such action could not only result in present injury, but also could undermine the competitive process that encourages innovation or maintenance of such facilities and thereby increase the risks of collateral consumer injury of a different type.⁷⁹

B. FTC Enforcement Under Section 5 Would Advance Consumer Sovereignty

The investigation of, and potential enforcement against, P2P software providers for the actions detailed above would advance the FTC’s core mission under Section 5 of safeguarding consumer sovereignty. “[T]he core of modern consumer protection policy is to protect consumer sovereignty by attacking practices that impede consumers’ ability to make informed choices”⁸⁰

The acts and practices described above involve a major compromise, if not a complete loss, of consumer sovereignty. In many instances, personally identifiable information is being transmitted to third parties without the consumer’s knowledge or consent. In other examples, programs like Altnet actually hijack existing capacity on a consumer’s computer, using it in ways to which the consumer neither intended nor consented. In all cases described above, the

⁷⁹ *In the matter of C&D Electronics, Inc.*, 109 F.T.C. 72 (1987) (Separate Statement of Chairman Daniel Oliver).

⁸⁰ Timothy J. Muris, *The Federal Trade Commission and the Future Development of U.S. Consumer Protection Policy*, Remarks at the Aspen Summit (Aug. 19, 2003).

deceptive practices of the P2P providers result in consumers, who often are teenagers or children, attempting to make choices in the digital marketplace in the face of drastically imperfect information. As consumer protection “generally can be thought of as policing the market against acts and practices that distort the manner in which consumers make decisions in the marketplace,”⁸¹ FTC investigation of the P2P providers’ business practices, and enforcement actions if warranted, are appropriate to protect consumers, especially this nation’s youth.

C. P2P Providers’ Business Practices May Also Violate the Children’s Online Privacy Protection Act

The collection, use, and disclosure of personal information from children by P2P providers also raises serious questions under the Children’s Online Privacy Protection Act of 1998 (“COPPA”).⁸² The FTC’s implementing regulations of this statute prohibit operators of Internet services directed to children, or operators that have actual knowledge that it is collecting personal information from a child, to collect personal information from children without first (i) providing information on what information it collects from children, how it uses and discloses this information; (ii) obtaining verifiable parental consent prior to any collection, use, or disclosure of such information from children; and (iii) providing a reasonable means for parents to review the personal information being collected from a child.⁸³

The COPPA’s application is broad. The personal information it seeks to protect includes name, address, e-mail address, and telephone number.⁸⁴ Simply collecting such information without parental consent, even without disseminating or using the information collected, is prohibited under the statute.⁸⁵ The COPPA defines a “child” as someone under the age of 13.⁸⁶

⁸¹ Timothy J. Muris, *The Interface of Competition and Consumer Protection*, Address at the Fordham Corporation Law Institute’s Twenty-Ninth Annual Conference on International Antitrust Law and Policy (Oct. 31, 2002).

⁸² 15 U.S.C. § 6502.

⁸³ See 16 C.F.R. 312.3.

⁸⁴ See *id.* at § 312.2.

⁸⁵ See *id.* at § 312.1.

Violations of the COPPA are punishable by the FTC as unfair or deceptive acts or practices under Section 5.⁸⁷

To determine whether a particular operator's Internet site is directed to children, the COPPA's implementing regulations require the FTC to "consider competent and reliable empirical evidence regarding audience composition."⁸⁸ Children are some of the primary users of P2P networks. While our preliminary analysis did not find empirical evidence directly quantifying the presence of all children on P2P networks, studies that have examined P2P demographics have included children – as defined under COPPA – in their age groups. For example, one study found that 56% of consumers age 12-17 had downloaded music – the highest percentage of any age group in the survey.⁸⁹ Another study found that 41% of respondents aged 12-17 are engaging in file-sharing on P2P networks.⁹⁰ Based on 2000 U.S. Census data, this translates to around 8.7 million Americans between the ages of 12 and 17. By far the most popular songs traded on P2P networks tend to be current "pop" hits popular with teenagers and children. For example, during the week ending April 12, 2004, the ten most downloaded tracks included Britney Spears' "Toxic" and Linkin Park's "Numb."⁹¹

Therefore, distributors of P2P software have constructive, if not actual, knowledge that a significant number of individuals downloading the software they distribute and using it to trade files over P2P networks are children as defined under the COPPA. Despite this knowledge, the major P2P distributors are not complying with the COPPA's strict requirements. For example,

⁸⁶ See 15 U.S.C. § 6501(1).

⁸⁷ See 16 C.F.R. § 312.9.

⁸⁸ *Id.* § 312.2.

⁸⁹ See Edison Media Research, The National Record Buyers Study II (June 2002).

⁹⁰ See Ipsos/Reid, File-Sharing and CD Burning Proliferate (June 12, 2002)

⁹¹ See www.bigchampagne.com/radio.html

parental consent is not required prior to a child downloading P2P software and trading files over P2P networks. During the downloading and/or file sharing processes, personal information (such as an e-mail address) is collected from all users, including children. The mere collection of such information from children without prior verifiable parental consent, even without its subsequent use or distribution, is a COPPA violation. The act of third-party adware/spyware providers of transmitting information collected from children may constitute a further violation.

In apparent attempts to avoid potential liability under COPPA, some P2P software providers apparently ignore usage by children, or otherwise disclaim liability. Despite the millions of young consumers using P2P networks, P2P software provider Morpheus claims that “Morpheus.com is a general audience site, and we do not knowingly collect information about children.”⁹² Further investigation would reveal how many children are, in fact, downloading the software provided by Morpheus. In paragraph 4 of its EULA, iMesh claims that children are prohibited from downloading its software, and that if iMesh discovers that a child has, in fact, downloaded its software, it terminates the child’s user agreement.⁹³ Further investigation would reveal how many copies of iMesh software have been downloaded by children and if, in fact, iMesh terminates these agreements.

In summary, perhaps the biggest ongoing violation of the COPPA – the collection and dissemination of personal information from millions of children throughout the United States without parental consent – is occurring right now over P2P networks. Consistent with its commitment that “the FTC is serious about enforcing the [COPPA],”⁹⁴ P2P networks warrant further investigation under the COPPA in addition to Section 5.

⁹² www.Morpheus.com/notices.html

⁹³ See iMesh EULA ¶ 4.

⁹⁴ FTC Press Release, “FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Violations” (July 21, 2000) (quoting former Bureau of Consumer Protection Director Jodie Bernstein).

VIII. CONCLUSION

The main activities, legal issues, and consumer injuries analyzed in this white paper are summarized in the chart attached on the following page. While by no means comprehensive, the chart makes clear that P2P providers are engaging in numerous activities that appear to violate the FTC Act and the COPPA and cause significant harm to consumers, many of whom are children. Absent an FTC investigation and enforcement action if P2P providers are violating the FTC Act and the COPPA, these practices will continue and the consumer injury will only escalate.

P2P CONSUMER PROTECTION ISSUES MERITING FTC INVESTIGATION

<u>Activity</u>	<u>Legal Issue</u>	<u>Consumer Harm</u>
<ul style="list-style-type: none"> ▪ Facilitating Spread of Viruses 	<ul style="list-style-type: none"> ▪ Deceptive/Unfair: Material omission of risk of use 	<ul style="list-style-type: none"> ▪ Degradation of computer functionality, including complete loss of use ▪ Harm to fellow network users (e.g., in business environments) ▪ Indirect/shared harm to all Internet users
<ul style="list-style-type: none"> ▪ Unwanted use of computer processor/bandwidth resources 	<ul style="list-style-type: none"> ▪ Deceptive/Unfair: Failure to disclose full cost of using product 	<ul style="list-style-type: none"> ▪ Degradation of computer processing and/or communications capability, including complete loss of use
<ul style="list-style-type: none"> ▪ Bundling Spyware 	<ul style="list-style-type: none"> ▪ False: Falsely claim “we do not bundle spyware” ▪ Deceptive: Material omission of fact that spyware is bundled ▪ Unfair: EULAs pass liability to consumers but fail to provide information on third party software ▪ COPPA: Spyware collects information about children without parental consent 	<ul style="list-style-type: none"> ▪ Degradation of computer functionality (e.g., through search-engine re-directors, unwanted pop-up ads) and possible requisition of computing capacity ▪ Increased spam e-mail ▪ Exposure of children to unwanted/inappropriate advertisements/content
<ul style="list-style-type: none"> ▪ Childrens’ Participation 	<ul style="list-style-type: none"> ▪ COPPA: P2Ps collect info without parental consent ▪ Lack of substantiation: P2Ps claim they revoke user licenses but they do not 	<ul style="list-style-type: none"> ▪ Exposure of children to unwanted/inappropriate advertisements/content
<ul style="list-style-type: none"> ▪ Failing to warn of user’s litigation risk 	<ul style="list-style-type: none"> ▪ Deceptive 	<ul style="list-style-type: none"> ▪ Exposure of consumers to litigation/damages ▪ Exposure of parents to litigation/damages incurred by their children

A Report to the Subcommittee on Courts, the Internet, and Intellectual Property
House Judiciary Committee
By the Joint Committee of the Higher Education and Entertainment Communities
On Progress during the Past Academic Year
Addressing Illegal File Sharing on College Campuses
August 2004

The 2003-2004 academic year saw significant change in approaches to accessing digital entertainment content on college and university campuses across the country. In light of the Subcommittee's requests for periodic updates, the Joint Committee of the Higher Education and Entertainment Communities is providing this report on the status of efforts to address the opportunities and challenges presented by digital copying and distribution of copyrighted works through peer-to-peer (P2P) file sharing networks and alternative means.

Colleges and universities continue to address these issues in several different ways, adopting new policies as well as technological and educational measures to maintain the integrity of the schools' networks while ensuring a convenient, protected, and legal environment in which legitimate offerings can thrive.

Legitimate Online Services

Colleges and universities have increasingly been offering new services and amenities to their students, such as free newspapers, special phone plans, and access to cable TV. Heeding the call for new sources of legal content, schools this past year began to introduce legitimate music services on campus.

In November of 2003, Penn State University signed an agreement with the now-illegitimate Napster for a pilot program. The service offered students free on-demand streaming audio and downloaded songs, with an option to transfer to a CD for an additional fee. The University of Rochester began offering the same service in February of this year. Fees are paid to the on-line services by the universities for this access, and the services then pay royalties to the copyright holders of the music according to negotiated agreements. Napster partnered with IBM on an affordable file server that can locate their entire cache of music on campus, using the university's internal networks and avoiding the need to use external bandwidth. Later this fall, Napster, in partnership with Microsoft, will launch an additional service that will allow students, for an add-on subscription fee, the opportunity to download their music to portable players.

With the success of these programs, many more schools will begin to partner with legitimate music businesses during this new academic year. For example, Napster recently announced agreements to offer similar programs at the University of Southern California, University of Miami, George Washington University, Cornell University, Middlebury College, Vanderbilt, and Wright State University. Additional companies have lined up to offer their services. After a well-received pilot at Yale this past year, Ctrax is planning to offer its subscription service and download store to at least 20 other

schools, including Wake Forest, Tulane, Purdue, and Ohio University. The service works through the university's local area network, and can incorporate features specifically tailored to each school, providing an outlet for locally produced music. Ctrax is based on its popular sister service, Cflix, which provided Yale, Duke, Wake Forest, and the University of Colorado with video-on-demand. The companies will combine their offerings of music and movies, as well as educational media services, under the name Cdigix, and will partner with more schools in the 2004-2005 academic year, including Marietta College, the Rochester Institute of Technology, and others.

This month, MusicRebellion begins offering a pay-per-download service to DePauw University. The service offers an interesting twist in that the price of individual songs will be driven by demand. In addition, students will receive a \$3 credit after completing an "education module," which gives an overview of music and the "ramifications of pirating media." The service is further integrated with the institution by allowing students to submit their own original music, and by donating 1% of sales to DePauw student scholarships.

Also this month, Northern Illinois University launched a service from Ruckus, offering legally downloaded music, streaming movies, and local content; and the University of California, Berkeley, and the University of Minnesota announced partnerships with RealNetworks to give students unlimited access to streamed music at a significantly reduced cost.

Finally, Apple has offered to colleges and universities a site license to its popular iTunes Music Store, and enabled the schools to purchase songs for their students at a discount. This fall, Duke will offer all incoming freshmen an iPod portable music device, enabling students to carry with them downloaded lectures and course materials, in addition to the songs acquired through iTunes.

This means that at least 20 different universities have already signed agreements to legally deliver entertainment content to students. This is an extraordinarily promising trend that will only continue in the coming academic year. These programs have garnered substantial attention and many schools, and even student groups, have formed task forces to determine whether legitimate services on campus are a viable alternative and which services may be right for them. We are even witnessing that some candidates for student government leadership positions are running on platforms that encourage university administrators to adopt on-line music services.

Campus Action Network (CAN), a music industry-wide effort led by Sony BMG Music Entertainment, and supported by other record companies, has worked over the past year to encourage the launch of legitimate music services on campuses around the country. CAN's efforts have been supported by the Joint Committee of the Higher Education and Entertainment Communities, with Co-Chair Graham Spanier making introductions to university presidents for representatives of CAN.

CAN provides universities with introductions, information, and support for a broad array of online music services. To support the launch of online campus music services in the fall of 2004, CAN is working with the services and schools to provide a wide range of campus marketing initiatives, such as on-campus concerts, artist appearances, contests and promotions. CAN is also collaborating with schools to explore how these services can be used for educational purposes.

Educational Initiatives

The 2003-2004 academic year began with many colleges and universities questioning their role in engaging students in a discussion of copyrighted works and the proper use of computer networks. There has been a sea change in perspective, however, and many schools have come to realize that they are uniquely positioned to educate on the value of copyright law and the safeguards it provides to authors, artists, and writers of creative works—works which often come from the school community itself. Messages, in emails and letters, have been sent from the highest administrative levels to ensure that students understand the significance of infringement on campus. These messages have been sent to staff and faculty as well, reminding them that penalties for illegal conduct are not just for students.

Dozens of colleges and universities—Indiana University, Brown University, and Dartmouth College, to name just a few—have made updates to their Acceptable Use policies to acknowledge and reflect the change in application of their school's resources. These policies can regularly be found online and in hard copy. Information is now more accessible than ever on subjects such as copyright, infringement, P2P file sharing, and the proper use of digital media. Students are also often required to engage in short tutorials and quizzes before acquiring access to networks in order to ensure their knowledge and understanding of appropriate use.

Administrations have distributed notices, posters, and fliers to convey the message that infringement is wrong—and that there are alternatives. Discussions, presentations, and even courses have been offered to engage the academic community in dialogue on these subjects.

Important educational initiatives are emerging from this collaboration between higher education, on-line services, and the entertainment industry. For example, music providers have offered to electronically distribute recordings of college and university orchestras, bands, and choral groups. At Penn State, on-line courses are being developed on topics such as popular culture that have direct links, for educational purposes, to certain recordings. Music students will have on-line access to music instead of having to visit the reserve music room of the library. Other creative uses are emerging.

Enforcement

While educational initiatives have grown, schools have sought to emphasize the importance and seriousness of the message through enforcement. First violations of

computer use policies, including single instances of infringement, have borne penalties ranging from simple warnings to mandatory informational sessions to temporary denial of network access. Second violations have carried stricter penalties, including discontinuance of network access to probation to notation on permanent records. Further violations, while increasingly rare, have carried penalties as serious as expulsion. New and creative means of enforcement are also being presented, such as fining students for notices of infringement.

For those students who have questioned the vigilance of their own schools, this past year has reminded them that responsibility does not wait for graduation. The much-publicized lawsuits by the music industry were brought to campuses as 158 students from 35 universities across the country found themselves accountable for their illegal actions.

Over the 2003-2004 academic year, schools implementing new infringement prevention programs and methods reported significant decreases in illegal file sharing and incidents of discipline for infringement. While several of the measures mentioned here have worked to bring about this change, the publicity of enforcement was often cited as the most important—and effective—element.

Technological Measures

More schools began this past year to complement these programs with different technological measures. Sometimes the call for these additional measures came from the students themselves. In one case, the Student Senate voted to block illegal trading after learning that illegal file sharing was responsible for bringing their university network to a crawl. Suffering from performance and reliability problems, decreased bandwidth, and the spread of viruses, schools have sought to free up their networks for their intended educational purpose.

Many schools—University of California, Berkeley, Penn State University, Vanderbilt University, and Central Michigan University, to name just a few—have limited students' bandwidth to a certain amount per week. When students exceed this limit, they are warned, and their network access is subject to being significantly reduced in speed or ultimately discontinued.

In June of 2003, the University of Florida introduced ICARUS, an application designed to address inappropriate use on the school's network. Since its inception, ICARUS has automatically processed 6,503 Acceptable Use Policy violations, including P2P violations. The system has had only five false positives out of 6,508 detected violations, and none of them was related to P2P activity. The school is now planning to license the system to other schools.

Some schools have complemented their networks with Audible Magic's CopySense system, which weeds out infringing transmissions on P2P networks. With CopySense installed, IT administrators have reported reclaiming half of their network's bandwidth at

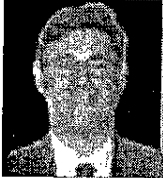
significantly reduced costs. One school went from at least one notice of infringement per week to none.

Conclusion

Colleges and universities are collaborative communities. In that spirit, many different segments of academia have contributed their views and perspectives on how higher education should address the issues posed by illegal file-sharing. Each year, university administrations experiment with the offerings and combinations that work best for them. Even more changes are likely in the coming years, based on the experiences gleaned from the efforts now being tried. We welcome these initiatives.

January 2004

eMarketer™ Spotlight Report



Ross Rubin, Senior Analyst
rrubin@emarketer.com

Digital Music:

"Fear-to-Peer" Tactics Pave Way for Download Revenue

Impetus: The latter half of 2003 has seen many new and revived entrants in the digital music space, including new offerings from BuyMusic.com, MusicMatch, MusicNow and Napster. Apple Computer, which pioneered the a la carte song download model with its iTunes Music Store, recently sold its 25 millionth legal digital song, and new entrants such as HP, Microsoft and Amazon.com are slated to appear in 2004. Are Internet users ready to forsake peer-to-peer services for the new breed of online music retailers?

Impact that Downloading "Free Music" Has on Actual Music Purchases in the US, 2003 (as a % of respondents)

Increased purchases of CDs/tapes by 50%+

15%

Increased by 25%

11%

Increased by 5-10%

11%

No Impact

52%

Decreased by 5-25%

4%

Decreased purchases of CDs/tapes by 50%+

7%

Source: Insight Research, September 2003

052790 ©2003 eMarketer, Inc.

www.emarketer.com

A. Overview	2
B. Digital Music Forecasts	4
C. Consumer Behavior	5
D. Digital Music Usage	6
E. Digital Music Demographics	10
Company Profile	12
F. Consumer Attitudes	13
eMarketer View	17
Related Information & Links	17

Core Topics

■ Consumer Online Content ■ North American B2C E-Commerce

Issues & Questions

- What have been the effects of recent RIAA lawsuits against consumers?
- What is the future importance of CDs, CD burning and portable digital music players?
- How can music retailers confront current attitudes regarding music sharing?
- What kind of impact will legal digital music have on piracy?

Analysis

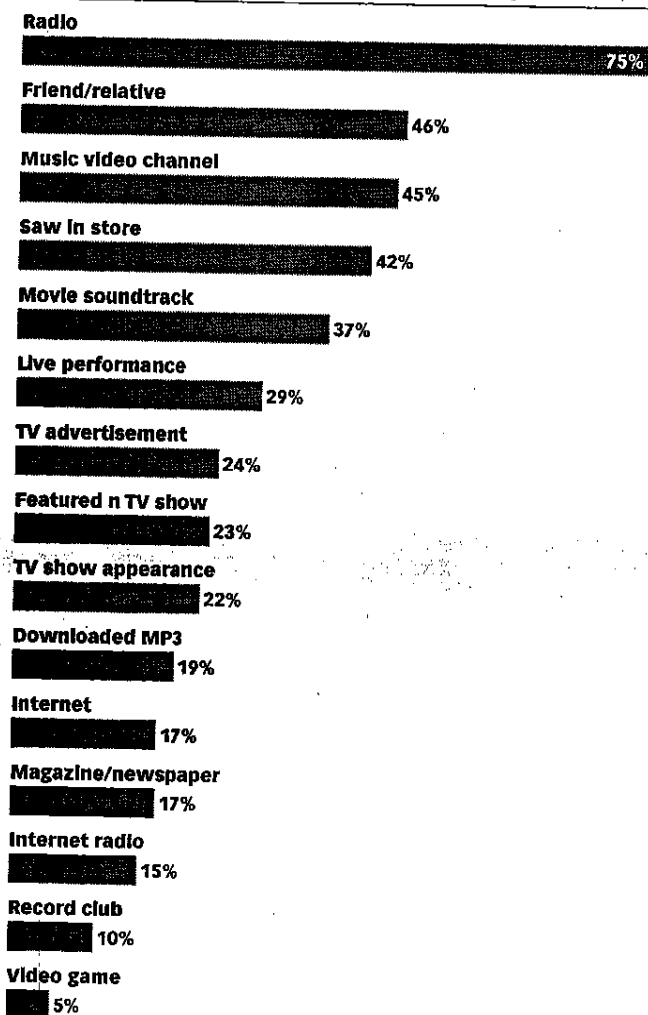
In the heyday of the original Napster, there was a popular belief that file sharing, or unauthorized downloading of music, would mean the death of the music industry. Napster, on the other hand, argued that illegal downloads were useful as a promotional tool. Indeed, data released by Insight Research long since the closure of that popular network shows that the majority of consumers report that downloading free music has no impact on their CD purchases, and 37% reported an increase in the purchase of CDs.



A. Overview

Edison Media Research also found that 19% of consumers who had purchased a CD in the past year had been influenced to do so by an MP3 download, and 17% by the Internet in general. While this influence is significant, it is far below other media such as radio and music video channels, word of mouth and live performances. However, MP3 downloads had a stronger influence than Internet radio. This kind of insight could prove useful to labels in evaluating subscription services, many of which offer Internet radio with more options.

Type of Media that Influenced US Consumers* to Purchase their Last CD, 2003 (as a % of respondents)



Note: *consumers who have purchased a music CD in the past 12 months
Source: Edison Media Research, June 2003

052697 ©2003 eMarketer, Inc.

www.eMarketer.com

However, declining CD sales have been the smoking gun that the Recording Industry Association of America (RIAA) used to insist that Napster and its ilk were damaging industry profits. CD sales have been in a precipitous decline since 2000, although revenue has not dipped as severely.

US Recording Industry Revenues, 1997-2002 (in millions)

Year	Revenue (in millions)
1997	\$12,236.80
1998	\$13,723.50
1999	\$14,584.50
2000	\$14,323.00
2001	\$13,740.89
2002	\$12,614.21

Source: Recording Industry Association of America (RIAA), 2003

054523 ©2003 eMarketer, Inc.

www.eMarketer.com

According to the RIAA, CDs garnered over \$12 billion in 2002 in the US; while that figure represents a drop from their peak in 2000, it puts Apple's run-rate of 75 million songs per year (at 99 cents per song) in perspective. Mid-2003 data from the RIAA confirms that CD sales continue to fall in the US. Units are off 15.3% while total dollars are down 11.8%. While CDs continue to constitute the overwhelming majority of formats, the legacy format of cassettes continues to drop sharply. Not all news was bad, however. CD singles, which piracy should have an adverse impact on, were up 162.4% from mid-2002, and DVDs of concerts and music videos were up 19.4%. However, DVD-Audio, one of the two copy-protected formats that the music industry hopes would succeed CDs, sold just 100,000 units and were down 49% from last year.

Music Manufactures Unit Shipments and Revenue, January-June 2002 vs. January-June 2003 (in millions)

	2002		2003		% change (revenue)
	Total units	Total revenue	Total units	Total revenue	
CD	369.1	\$5,243.90	312.6	\$4,623.10	-11.8%
Cassette	16.7	\$112.00	8.1	\$47.50	-54.3%
CD single	2.2	\$8.90	5.8	\$5.80	173.5%
DVD video	4.6	\$105.80	5.6	\$133.50	26.2%

Source: Recording Industry Association of America (RIAA), August 2003

054524 ©2003 eMarketer, Inc.

www.eMarketer.com

A. Overview

If the economy continues to improve in 2004, it may shed light on the impact of the economic downturn that coincided with the drop in CD sales; many of those who questioned the impact of Napster cited the recession as a leading cause of the music industry's woes. Even if the CD decline has been primarily due to piracy, however, not all downloaders download equally. Edison Media Research has found that the likelihood of purchasing less music corresponded with the number of files a respondent had downloaded. Nearly half of those who had downloaded more than 100 files said they had purchased less music. However, only 36% of those who had purchased fewer than 100 files said they purchased less music, a percentage close to the 34% of non-downloaders who had also purchased less music.

US Downloaders and Non-Downloaders Who Say that They Have Purchased Less Music in the Last 12 Months, by Number of Files Downloaded, 2003 (as a % of respondents)

Downloaded 100+ files	49%
Downloaded <100 files	36%
Non-downloaders	34%

Source: Edison Media Research, June 2003

052689 ©2003 eMarketer, Inc.

www.eMarketer.com

Around the time of Napster's demise, the major labels responded with a pair of legal music subscription sites. MusicNet, which continues to serve AOL, was to be a digital music wholesaler and systems integrator, while PressPlay, which formed the basis for the new Napster, was to be a retailer. However, initial offerings from both camps were criticized as expensive, with limited selection and restrictive song usage. In their initial incarnations, they relied heavily on "tethered" downloads to which subscribers lost access if they cancelled the service. Napster and RealOne Rhapsody continue to offer tethered downloads, although Napster provides the option of making them more permanent.

"The music industry has been spoiled. They have controlled the distribution of music by producing CDs, and thereby have also protected their profits. So they have resisted Internet distribution. The music industry has to reinvent itself. We can no longer control distribution the way we used to." *Nobuyuki Idei, CEO, Sony*

While its initial selection was also relatively small at only 250,000 songs (it has since expanded to 400,000), Apple's iTunes Music Store found success selling songs at 99 cents and most albums at \$9.99 with no subscription required. Apple's entrance has spurred a slew of old and new entrants to revamp their offerings even though the company repeatedly insists that it does not expect to make major profits by selling online music. Rather, it sees the availability of digital music as a hook for consumers to purchase its popular but pricey iPod portable digital music player. The iPod is the only player that supports iTunes' digital rights management (although iTunes can burn protected tracks to CDs), and iTunes is the only digital music store that the iPod supports (although it can also play unprotected MP3 files).

While both iTunes and the iPod have led their respective revenue categories for months, it will be difficult for the company to compete with an increasing number of hard-disk-based portables that use the Windows Media format supported by BuyMusic.com, MusicMatch, Napster and others. Napster 2.0 claims to support more than 40 digital music players.

B. Digital Music Forecasts

In August 2003, Forrester Research estimated that the music industry has already lost \$700 million due to peer-to-peer networks, and that by 2008, CD sales would be down 30% from their 1999 peak. According to Informa Media Group, losses from peer-to-peer networks are expected to continue to nearly double from 2003 to 2008, when it expects labels to lose \$4.7 billion to such file sharing.

Lost Music Sales due to P2P-Style Networks Worldwide, 2003 & 2008 (in billions)



Source: Informa Media Group, September 2003

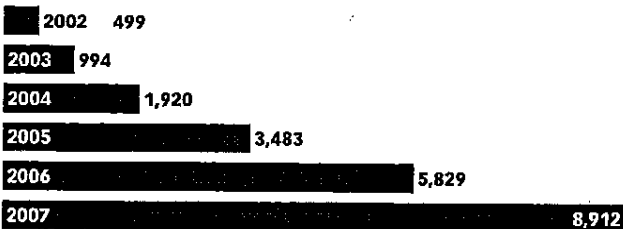
052393 ©2003 eMarketer, Inc.

www.eMarketer.com

“Remember there are 10 billion songs that are distributed in the US every year legally, on CDs. So we’re at the very beginning of this. It will take years to unfold.” Steve Jobs, CEO, Apple Computer

More music services, such as BuyMusic.com and MusicMatch Downloads, enable consumers to purchase digital music tracks without paying a monthly fee. Furthermore, Loudeye, which encodes music for Apple and other stores, announced that it would offer a private-label digital music store to the likes of AT&T. However, digital resellers must license their own catalogs. Nonetheless, analysts have projected that subscription services will attract members. In December 2002, IDC projected that total paid music subscription households would grow to over 11 million in 2006. More conservatively, GartnerG2 believes there will be over 5.8 million subscribers in the US by that time.

Online Music Subscribers in the US, 2002-2007 (in thousands)



Source: GartnerG2, April 2003

051754 ©2003 eMarketer, Inc.

www.eMarketer.com

Given the early stage of the legal digital music market, it is not surprising that market size estimates vary widely. For 2003, estimates ranged from \$16.9 million by US Bancorp Piper Jaffray to \$800 million by Jupiter Research. For 2006, GartnerG2’s revenue estimate is nearly triple that of Piper Jaffray’s, and Jupiter’s projection for 2008 is more than six times that of Piper Jaffray’s.

Comparative Estimates: Online Music Revenues in the US, 2002-2008 (in millions)

	2002	2003	2004	2005	2006	2007	2008
Gartner G2, February 2003	\$29.5	\$89.5	\$174.7	\$329.7	\$618.2	-	-
International Data Corporation (IDC), December 2002	\$45.5	\$150.3	\$384.3	\$771.6	\$1,211.8	-	-
Jupiter Research*, July 2003	-	\$800	-	-	-	-	\$3,300
US Bancorp Piper Jaffray, September 2003	-	\$16.9	\$104.0	\$127.9	\$236.7	\$390.5	\$535.0

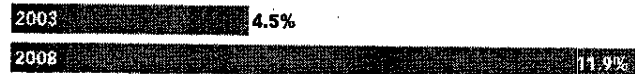
Note: *Includes online CD sales, digital downloads and digital subscriptions
Source: various as noted, 2003

054525 ©2003 eMarketer, Inc.

www.eMarketer.com

Informa Media Group believes that digital music will become a significant part of the music industry in 2008, when it is expected to grow from just 4.5% of sales in 2003 to 11.9%. In terms of industry impact, Informa’s estimate would appear to be on target with Jupiter Research’s 2008 revenue estimate of \$3.3 billion, which, if one assumes shrinking music company revenues, would allow digital music revenue to capture a double-digit share of the market.

Online Music Sales Worldwide, 2003 & 2008 (as a % of total music sales)



Source: Informa Media Group, September 2003

052392 ©2003 eMarketer, Inc.

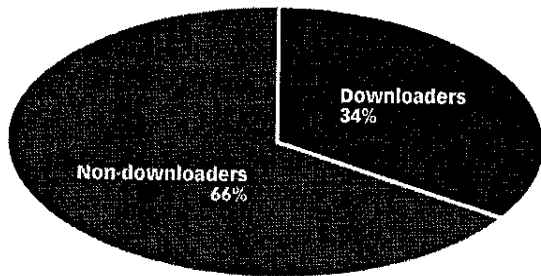
www.eMarketer.com

Forrester Research is even more bullish on the potential of digital music, projecting that, by 2008, 33% of music sales will come from downloads.

C. Consumer Behavior

At least prior to RIAA lawsuits against consumers, downloading digital music was an increasingly popular activity in the US. eMarketer estimates that 34% of US Internet users have download music in the past 12 months, for a total of 55 million users.

US Internet Users Who Have Downloaded Music in the Past 12 Months, 2003 (as a % of total internet users)



Source: eMarketer, December 2003

054526 ©2003 eMarketer, Inc.

www.eMarketer.com

While it is not yet as popular as sharing pictures or the nearly universal application of e-mail, its usage has increased from 35% in 1999 to 44% in 2002, according to Ipsos-Reid. Most studies find that at least 3 in 10 users have downloaded music, with all studies reporting a steady increase.

Comparative Estimates: Percent of Internet Users in the US Who Have Download Music, 2000, 2002 & 2003

	2000	2002	2003
eMarketer, December 2003	-	-	34.0%
Ipsos-Reid, March 2003 (1)	-	18%	-
Yankee Group, May 2003 (2)	-	-	32.0%
Pew Internet & American Life Project, July 2003 (3)	22.0%	29.0%	29.0%
International Data Corporation (IDC), December 2003 (4)	-	39.5%	-

Note: (1) n=1,112 Internet users surveyed in December 2002 that downloaded "in the past month." (2) Dial-up users only; 52% of broadband users download music; (3) n=1,555 music downloaders ages 18+ who have been online for less than a year (4) n=500 internet users with internet access at home

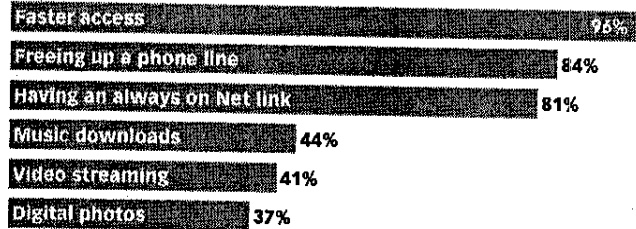
Source: various as noted, 2003

054527 ©2003 eMarketer, Inc.

www.eMarketer.com

ISPs have also been a target of the RIAA, and research shows they may have benefited from illegal downloading. Strategy Analytics has found that music downloads can be a powerful incentive to migrate to broadband. In fact, while most data shows that consumers are more actively exchanging digital photos than downloading music, 44% of those surveyed by Strategy Analytics cited music downloading as the most popular media-related reason for migrating to broadband.

Most Important Factors for Subscribing to Broadband according to US Broadband Subscribers, May 2003 (as a % of respondents)



Note: n=525

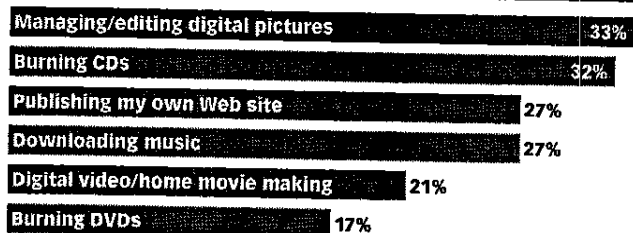
Source: Strategy Analytics, June 2003; Boston.com, June 2003

051440 ©2003 eMarketer, Inc.

www.eMarketer.com

InsightExpress has found that downloading music was an activity that 27% of home PC users wanted to spend more time doing. However, an even greater percentage (32%) said that they wanted to do more CD burning. While the percentage difference is not huge, the study suggests that what consumers want to do with digital music is more important to them than how they acquire it.

Computer Activities Home PC Owners in the US Want to Spend More Time Doing, July 2003 (as a % of respondents)



Note: n=500

Source: InsightExpress, July 2003

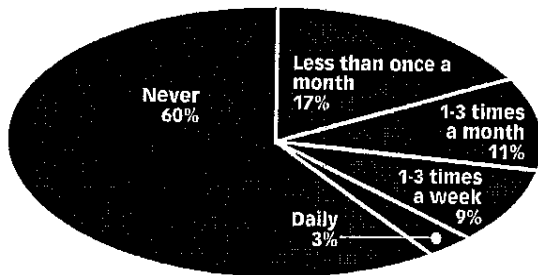
051247 ©2003 eMarketer, Inc.

www.eMarketer.com

D. Digital Music Usage

Data from Parks Associates indicates that digital music piracy is hardly an epidemic. Three in five households said they never use file-sharing applications. Of those households reporting using a music-sharing service, only 9% said they use such a service 1 to 3 times per week, and only 3% reported daily usage. These results are not promising for subscription services, which increase their value with frequent usage.

How Often US Internet Users Use File Sharing Applications, 2003 (as a % respondents)

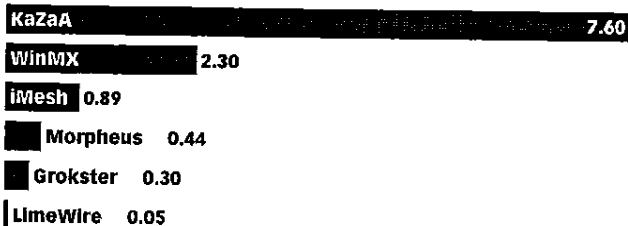


Note: n=5,592
Source: Parks Associates, 2003
054528 ©2003 eMarketer, Inc.

www.eMarketer.com

One tactic that the RIAA has tried in stopping free file-sharing services has been legal action against such services. This approach was effective in shutting down Napster. However, as was predicted, a number of new file-sharing services emerged in Napster's wake; KaZaA is, by far, the most popular of these. Since different parts of the company are scattered around the globe, KaZaA has been a harder legal target for the RIAA.

US Home Computers Actively Sharing Files, by Application, May 2003 (in millions)



Source: comScore Media Metrix, 2003; New York Times, September 2003
052034 ©2003 eMarketer, Inc.

www.eMarketer.com

Different file-sharing programs use different networks. LimeWire, for instance, uses the Gnutella network, which, unlike the old Napster, has no central directory of servers and is also better protected against copyright infringement lawsuits. Napster argued that it had no control over what kind of content was put on its servers, but as data from Prelude Systems shows, a miniscule percentage of files on the Gnutella network are legal files.

P2P Music Download Requests on Gnutella Network, by Material Type, February 2003 (as a % of requests surveyed)



Source: Palsade Systems, March 2003

048179 ©2003 eMarketer, Inc.

www.eMarketer.com

The vibrancy of file sharing networks depends on consumers' willingness to share their files. The Pew Internet and American Life Project found that 17% of US Internet users downloaded without allowing uploads; these users are called "leeches" on file-sharing networks. However, 12% participate fully in the networks by downloading and allowing uploading.

Attitudes of US Internet Users toward Downloading Music and Video Files, March-May 2003 (as a % of respondents)

Download music and video files and allow others to download files from their computers

12%

Download themselves, but do not allow others to download from their computers

17%

Allow others to download from their computers, but do not download themselves

9%

Do neither

62%

Source: Pew Internet & American Life Project, July 2003

051350 ©2003 eMarketer, Inc.

www.eMarketer.com

Another tactic that the RIAA has tried has been suing consumers directly. If the aim of this campaign was to dissuade the most egregious downloaders today, the trade association has missed its target. eMarketer believes that the consumer lawsuits, with their severe penalties, have been less effective in dissuading serious pirates than in causing mostly naive casual downloaders to panic.

D. Digital Music Usage

According to the NPD Group, 1.4 million households deleted all the digital music files saved on their PC hard drives in August 2003, a much higher number than in previous months. In May 2003, just 606,000 households deleted all digital music files from their PCs for reasons that may have included upgrading to archiving onto CDs. However, while the RIAA struck fear into the hard drives of some downloaders, their efforts did not have a huge immediate impact on piracy; 80% of the consumers who deleted files had fewer than 50 files saved; just 10% had more than 200 files.

In a September 2003 survey, NPD found that 40% of those who had downloaded from peer-to-peer networks said the lawsuits caused them to have a more negative opinion of the music industry. While eMarketer agrees with NPD and others that consumer lawsuits have generated considerable resentment toward the RIAA and possibly even the labels, this reaction is a red herring; consumers will not retaliate by purchasing less music. Consumers buy music to enjoy the work of artists, who have by and large wisely stayed in the background of the copyright infringement controversy. Music fans will be loath to deprive themselves in protest; this will outweigh any general ill will toward the recording industry, especially over time. The scattered boycotts by consumers will last only as long as they can keep the latest catchy tune out of their heads.

Indeed, the RIAA may have made an effective pre-emptive strike. It has delivered its public relations bombshell while broadband penetration is still relatively low. Had it delayed the extreme measure of suing consumers by several years, a new wave of broadband users would likely engage in more unauthorized downloading than they will now. Even so, if the RIAA does not continue its aggressive legal campaign against consumers, the impact of its actions in 2003 may be forgotten by 2005.

"So far, the RIAA's litigation has focused on users with the largest numbers of files to be shared, but it appears that the lawsuits are also having an effect on those with fewer files, indicating that the message that file sharing is illegal is getting through to mainstream consumers." *Russ Crupnick, Vice President, NPD Music*

In examining the effect of the RIAA's lawsuits against consumers, NPD found that the number of households acquiring music files reached a high of 14.5 million in April of 2003, but fell to 12.7 million households the following month and declined again in June to 10.4 million households. NPD later found that the number of households acquiring digital music via peer-to-peer file-sharing services declined by 11% from August to September 2003. During that same time period, the total number of music files downloaded decreased 9%.

Supporting the trend in NPD data, Nielsen/NetRatings found that usage of leading peer-to-peer application KaZaA fell a dramatic 41% between 29 June and 21 September 2003

Select File-Sharing Application Usage by Home Internet Users in the US, 29 June 2003 & 21 September 2003 (unique audience in thousands and % growth)

	29 June 2003	21 September 2003	% growth
KaZaA	6,526	3,867	-41%
Morpheus	272	261	-4%
iMesh	255	-	-
BearShare	192	-	-

Source: Nielsen/NetRatings, September 2003

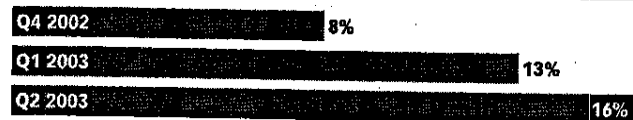
053455 ©2003 eMarketer, Inc.

www.eMarketer.com

This is not to say that the RIAA has ignored organized pirates, but much of its activity toward high-volume copyright violators has been aimed at those who profit from reselling pirated CDs in flea markets rather than online markets. In October 2003, the trade organization announced that it had seized approximately 2.5 million counterfeit CDs burned onto recordable media in the first six months of 2003, an increase of 18.1% from almost 2.1 million seizures at mid-year 2002.

In contrast to the decline in downloading at large, Ipsos-Insight has found that the number of US downloaders who have made a fee-based digital music acquisition doubled from 8% in the last quarter of 2002 to 16% in the second quarter of 2003.

US Music Downloaders Who Have Made a Fee-Based Digital Music Acquisition, Q4 2002-Q3 2003



Note: n=294 in Q4 2002, 337 in Q1 2003 and 269 in Q2 2003
Source: Ipsos-Insight, June 2003

053955 ©2003 eMarketer, Inc.

www.eMarketer.com

D. Digital Music Usage

Under Congressional scrutiny, the RIAA said that it would focus on those consumers who were aggressive downloaders. NPD Group, which uses software to determine the actual number of music files on consumers' PCs, has found that only about 16% of downloaders have over 500 songs on their computers. The research firm estimates that about two-thirds of music on consumers' PCs is downloaded as opposed to copied from CDs that consumers own.

Digital Music File Inventory Size per Household among US Downloaders, 2003 (as a % of respondents)



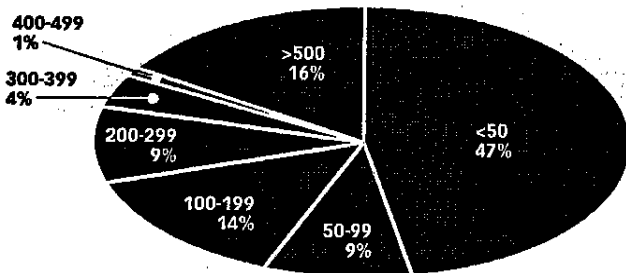
Source: NPD Group, September 2003

052189 ©2003 eMarketer, Inc.

www.eMarketer.com

Parks Associates data is remarkably consistent with that of NPD. The residential technologies researcher also found that 16% of US households had 500 or more songs stored on their PCs, while nearly half have fewer than 50 songs on their PC.

Number of Music Files Stored on PCs among US Households, 2003 (as a % respondents)



Note: n=297 households

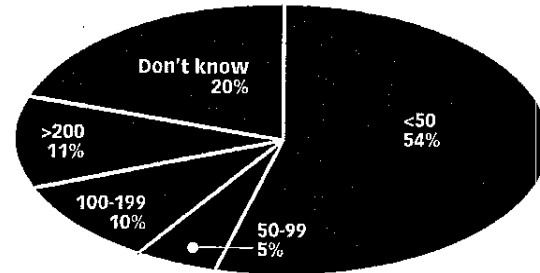
Source: Parks Associates, 2003

054529 ©2003 eMarketer, Inc.

www.eMarketer.com

One criticism of early file-sharing services was that they did not allow tracks to be burned to CDs. Ipsos-Reid has found that 34% of consumers had burned a CD of downloaded music in 2002. Despite the increased availability of bundled software such as Windows Media Player and iTunes that streamline the CD-creation process, Parks Associates data shows that more than half of households using digital music burned fewer than 50 songs to CDs. Assuming an average of 12 songs per CD, this equates to slightly more than four CDs per household. However, the 20% of digital music households that reported not knowing how many songs they had burned may include high-volume CD creators who have lost track.

Number of Music Files Burned to CDs among US Households, 2003



Source: Recording Industry Association of America (RIAA), 2003

054530 ©2003 eMarketer, Inc.

www.eMarketer.com

While audio CD burning may not yet be mainstream, it is easy to see why consumers would want to ensure compatibility with CD players. According to Yankee Group, many devices that can play CDs remain popular, particularly with younger consumers who have flocked to digital music. Portable CD players were owned by 82% of teens and were the most popular device among that group; 72% had a home CD player. More than half of teens had PCs and 45% had a DVD player, both of which can play CDs. Finally, 35% had a CD burner.

Among 18 to 24 year olds, penetration of most CD-compatible devices was even higher. 83% had a home CD player while 74% had a portable CD player, and at least 72% had a DVD player or PC. Young adults also reported substantially higher ownership of CD burners and car CD players. Young adults are more likely than teens overall to have cars, and CD players have become standard equipment on more automobiles, especially inexpensive models targeted at younger buyers. Chevrolet's new entry-level Aveo, which is available for under \$10,000, comes standard with an MP3-compatible CD player. In-car digital music is poised to become even more sophisticated. New products such as Rockford Fosgate's OmniFi offer in-car MP3 players that can synchronize the song collections on their hard disks with a home PC via Wi-Fi.

D. Digital Music Usage

Consumer Electronics Ownership among US Teens and Young Adults, by Age and Device, 2003 (as a % of respondents)

Portable CD player



TV set



Home CD player



VCR



PC



DVD player



Mobile phone



CD burner



Car CD player



Digital camera



■ Age 13-17

■ Age 18-24

Source: Yankee Group, August 2003

052001 ©2003 eMarketer, Inc.

www.eMarketer.com

While some newer DVD and CD players can read CDs filled with MP3 files instead of standard CD tracks (which allows them to hold approximately 10 times the amount of music), maintaining compatibility with these devices generally means limiting the CD's capacity. In contrast, hard-disk-based players like Apple's 40 GB iPod can hold up to 10,000 songs.

In September 2003, Parks Associates found that only 20% of US households that use digital music own an MP3 player. In addition, the installed base of portable music players may not be growing that quickly. The Consumer Electronics Association reports that only 16% of surveyed consumers planned to purchase a portable MP3 player during the 2003 holiday season. This was a significantly lower number than digital cameras, which are also related to PCs and sell at similar price points.

One reason for the disparity may be that there are more options for using a digital camera by the less technologically sophisticated. More color printers can now read flash memory cards or connect to a digital camera, circumventing a PC. For those who'd rather not print at home, photo processing labs and self-service stations at drug stores also accept memory cards from digital cameras. In contrast, portable MP3 players have almost no value without a PC with digital music files on it.

Consumer Electronics Likely To Be Purchased as Holiday Gifts In the US, 2003 (as a % of respondents)

DVD players



Digital cameras



Video gaming systems



Wireless phones



Portable MP3 player



Desktop, laptop or notebook computer



HDTV



Source: Consumer Electronics Association (CEA), October 2003

052937 ©2003 eMarketer, Inc.

www.eMarketer.com

"You've got a portable music player that can fit 10,000 songs on it? Come on. No one will spend \$1 a track filling it." Sean Ryan, Vice President Music Services, RealNetworks

However, Jupiter Research is optimistic about the prospects for portable MP3 players. In December 2003, Jupiter forecasted that US shipments of MP3 players will nearly double in 2003 to over 3.5 million, and will continue to grow almost 50% per year until 2006. Jupiter also sees promise in hard disk-based players and marks 2004 as the year they will surpass those based on flash memory. By 2006, Jupiter believes there will be more than 26 million MP3 players in use.

E. Digital Music Demographics

In looking at historical data collected by the Pew Internet and American Life Project from 2000 to 2003, a number of notable points emerge. As expected, younger Internet users (between 18 and 29) are the group that is most likely to download music. While education became a less important predictor of music downloading activity in 2003 than it had been in 2002, Internet user experience became more important, with 59% of those who had been online more than three years downloading music.

Profile of Music Downloaders in the US, 2000-2004 (as a % of respondents)

	July-August 2000	February 2001	March-May 2003	November-December 2003
All adults	22%	29%	29%	14%
Men	24%	36%	32%	18%
Women	20%	23%	26%	11%
Whites	21%	26%	28%	13%
Blacks	29%	30%	37%	25%
Hispanics	35%	46%	35%	20%
Age				
18-29	37%	51%	52%	28%
30-49	19%	23%	27%	13%
50+	9%	15%	12%	6%
Household Income				
<\$30,000	28%	36%	38%	22%
\$30,000-\$50,000	24%	31%	30%	15%
\$50,000-\$75,000	20%	29%	28%	12%
\$75,000+	15%	24%	26%	16%
Educational attainment				
Less than high school	38%	55%	39%	24%
High school graduate	25%	31%	31%	18%
Some college	25%	32%	33%	13%
College degree or more	15%	21%	23%	11%
Internet user experience				
<6 months	20%	27%	26%*	16%*
6 months to 1 year	20%	25%	26%*	16%*
2-3 years	24%	28%	29%	12%
3+ years	22%	33%	59%	15%
Home broadband users				
	-	-	41%	23%
Full and part time students				
	-	44%	56%	24%

Note: *represents music downloaders who have been online for less than a year

Source: Pew Internet & American Life Project, January 2004

051351 ©2003 eMarketer, Inc.

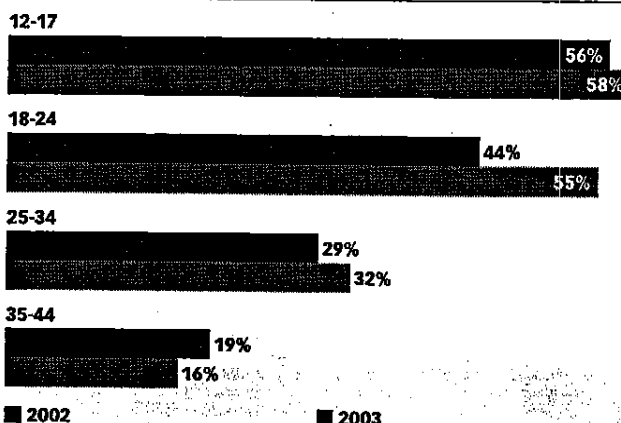
www.eMarketer.com

Music downloading has been traditionally associated with younger consumers for a variety of reasons:

- Their greater consumption of music in general
- Their embrace of popular music that is most readily accessible on peer-to-peer networks
- Their high usage level of the Internet and social activity online
- Their relatively high leisure time, often limited incomes, and, in college environments, high-speed Internet connections.

Data by Edison Media Research shows that the number of online music downloaders increased between 2002 and 2003 across users aged between 12 and 34, particularly among the 18-24 group.

US Online Music Downloaders, by Age, 2002 & 2003 (as a % of respondents in each group)



Source: Edison Media Research, June 2003

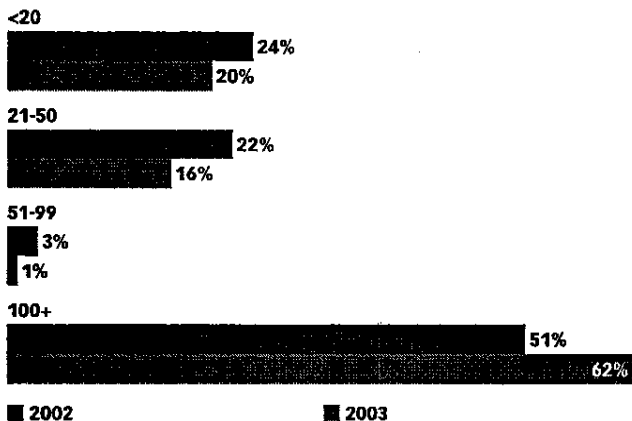
052682 ©2003 eMarketer, Inc.

www.eMarketer.com

E. Digital Music Demographics

Edison Media Research also found that a far greater percentage of downloaders ages 18 to 24 appear to be music hoarders. A striking 62% of music downloaders surveyed by Edison Media Research reported having downloaded 100 or more songs over the Internet, up from 51% in 2002. This is in contrast to data from both NPD and Parks Associates that shows that fewer than 45% of consumers overall had more than 100 songs on their PCs.

Average Number of Songs Downloaded over the Internet by US Downloaders Ages 18-24, 2002 & 2003 (as a % of respondents)



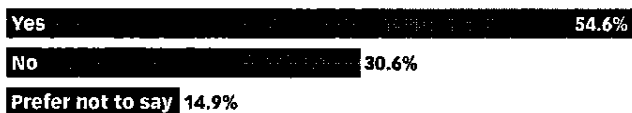
Source: Edison Media Research, June 2003

052685 ©2003 eMarketer, Inc.

www.eMarketer.com

The National Association of College Stores (NACS) found that over half of college students download music from the Internet for free. Nearly 15% of respondents preferred not to say whether they downloaded, indicating a lack of openness regarding their downloading habits.

US College Students Who Download Music from the Internet without Charge, 2002 (as a % of respondents)



Source: Student Watch from the National Association of College Stores (NACS), August 2003

051833 ©2003 eMarketer, Inc.

www.eMarketer.com

Many of those who did not respond to the NACS study may in fact be downloaders, though. When college students were asked a similar question by Ipsos-Reid one month later regarding downloading habits, about the same percentage of respondents said they did not download, but the percentage who said that they did was almost the same as those who answered yes plus those who offered no response to the NACS survey.

US College Students Who Have Downloaded Music Online or from P2P Programs, May-June 2003 (as a % of respondents)



Note: n=1,000

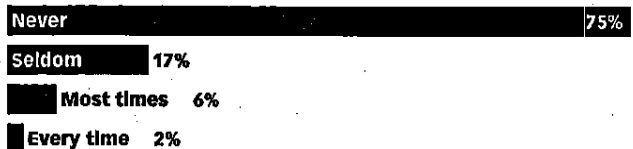
Source: Ipsos Public Affairs, September 2003

052404 ©2003 eMarketer, Inc.

www.eMarketer.com

Among US college students, Ipsos Public Affairs found that between May and June of 2003, three-fourths had never paid for music online, although 17% reported doing so at least occasionally, and 8% said they paid most times or every time. The days of unfettered access to peer-to-peer networks on campuses may be waning, however. Colleges are blocking access in response to RIAA lawsuits and, in November 2003, Pennsylvania State University announced it would make the new legal Napster service (see company profile) available to students at no charge; the agreement does not, however, include permanent downloads.

US College Students Who Pay for Music Downloaded Online or from P2P Programs, May-June 2003 (as a % of respondents)



Note: 69% of the 1,000 respondents say they download music

Source: Ipsos Public Affairs, September 2003

052405 ©2003 eMarketer, Inc.

www.eMarketer.com

Company Profile

Will Napster 2.0 Be The Cat That Eats The Apple?

While Apple's iTunes service is grabbing most of the headlines for now, one of the newest digital music services to debut has a name with a storied past. Napster was the software that ignited the peer-to-peer controversy by allowing consumers to share digital music files. The RIAA sued to close Napster and succeeded in shutting the service down in 2001.

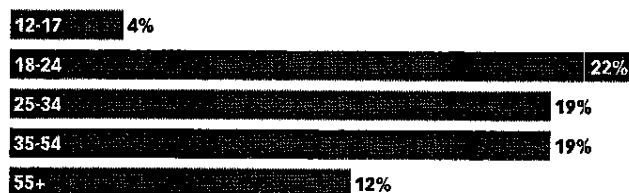
Now owned by Roxio, formerly best known for its CD-burning software, the new Napster is the result of putting an old moniker on what the company built from its recently acquired PressPlay service. Roxio is estimated to have paid about \$5 million for the Napster name and another \$39.5 million for PressPlay in May 2003. Formed by Sony Music and Vivendi Universal, PressPlay was one of the two original digital music services launched by the major labels. As such, the new Napster has little in common with its namesake aside from its feline logo. While users can create shared playlists, there is no peer-to-peer file sharing and all music is properly licensed.

If iTunes embodies the Macintosh philosophy of integration, Napster represents the Windows philosophy of choice. The new Napster offers over 500,000 songs (the most of any service), works with 40 different digital music players (including a hard disk-based model co-branded with Samsung), and offers two ways to acquire music. For \$9.95 per month, Napster's entire catalog, plus 45 radio stations, are available on demand. However, those wishing to download and burn tracks must still pay 99 cents per track or \$9.95 per album, the same prices that Apple charges. While the company doesn't promote it, it is possible to purchase songs without subscribing.

In a move to integrate more with the physical world, Napster offers a gift card that allows the purchase of 15 tracks. Digital music gift cards may prove popular; Apple has reported selling \$1 million worth of iTunes gift certificates since their launch in October 2003.

Younger Internet users have been identified as a particularly difficult market to migrate to paid services because of the notion that they do not believe file sharing is illegal or wrong. According to Ipsos-Insight, 18 to 24 year olds have been the most likely to purchase digital music online, although older users were not far behind. At this stage in market development, though, the general early adoption of that age group may distort long-term purchase behavior tendencies.

US Music Downloaders Who Have Made a Fee-Based Digital Music Acquisition, by Age, 2003



Note: 12-17: n=50; 18-24: n=72; 25-34: n=58; 35-54: n=67; 55+: n=13
Source: Ipsos-Insight, June 2003

053954 ©2003 eMarketer, Inc.

www.eMarketer.com

F. Consumer Attitudes

The RIAA has been relatively quick to draw its legal guns on consumers. Its critics offer that the recording industry has not made enough of an effort to educate the public on appropriate fair use. According to Newsweek, however, in the aftermath of consumer lawsuits, the majority of consumers surveyed believed that downloading music without paying was stealing, although a third still believed it did not constitute stealing.

US Consumers that Consider Downloading Music without Paying to Be Stealing, September 2003 (as a % of respondents)



Note: n=1,004
Source: Newsweek, September 2003

052203 ©2003 eMarketer, Inc. www.eMarketer.com

E-Poll also found that more consumers believed it was wrong to download files after the RIAA lawsuits. The impact was greatest on teens when it came to music, with 32.6% of those aged 13 to 17 believing that downloading without permission was wrong in October, up from only 20.2% in April. The RIAA's actions may have helped its motion picture counterpart, the MPAA. More teens and respondents at large felt it was wrong to download a feature film after the RIAA actions, although teens did not change their opinions quite as dramatically as they did for music.

US Consumers Who Believe It Is Wrong to Download Music or Feature Films without Artist/Label Permission, April 2003 & October 2003 (as a % of respondents)

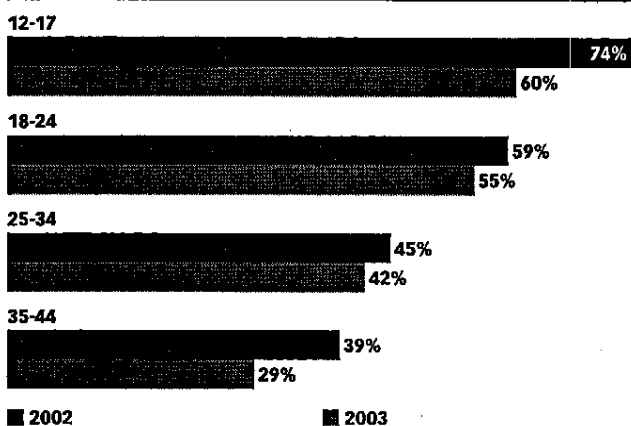
	All respondents		Teens 13-17	
	April 2003	October 2003	April 2003	October 2003
Music	42.8%	47.4%	20.3%	32.6%
Feature film	50.1%	57.2%	39.6%	48.5%

Note: April 2003 n=1,075 ages 13+; October 2003 n=1,162 ages 13+
Source: E-Poll, November 2003

053464 ©2003 eMarketer, Inc. www.eMarketer.com

Similarly, Edison Media Research found that the percentage of consumers who feel that there is nothing wrong with downloading music for free over the Internet decreased with age. While all age groups exhibited more sensitivity to copyright, the biggest impact was again among younger users. While 74% of those 12-17 saw no wrong in downloading free music in 2002, that number had been reduced to 60% in 2003. Nonetheless, even this reduced number represents a majority in the age group and remains higher than it is in any other age group.

US Consumers* Who Feel that There is Nothing Morally Wrong with Downloading Music for Free over the Internet, by Age, 2002 & 2003 (as a % of respondents in each group)



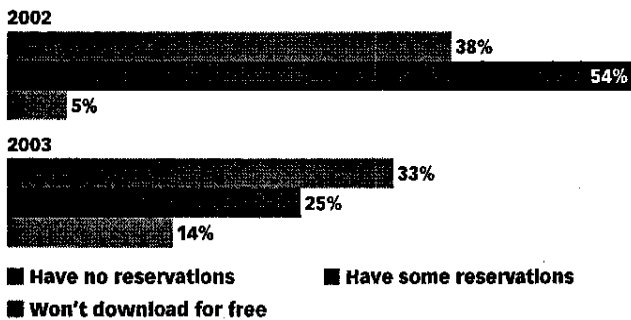
Note: *consumers who have purchased a music CD in the past 12 months
Source: Edison Media Research, June 2003

052691 ©2003 eMarketer, Inc. www.eMarketer.com

F. Consumer Attitudes

Consumers' attitudes affect their behaviors, but don't dictate them. Many consumers continue to download, but more may be on the verge of quitting. Comparing the attitudes of consumers from 2002 and 2003, Edison Media Research found that far fewer consumers were ambivalent about downloading; some of the fence sitters, however, had decided not to download free music, with that percentage growing from 8% to 14%.

Attitudes of US Downloaders toward Downloading Files for Free over the Internet, 2002 & 2003 (as a % of respondents)



Source: Edison Media Research, June 2003

052692 ©2003 eMarketer, Inc.

www.eMarketer.com

indeed, the RIAA lawsuits played upon what seemed to be the dominant deterrent to downloading, according to Forrester Research. In surveying young consumers aged 13-30, Forrester found that 68% a very high percentage of these consumers, traditionally heavy downloaders, would stop if there were a serious threat of legal action. In contrast, longer wait times would deter only 30% of consumers. Little variation existed throughout the spectrum of teenage years.

Attitudes toward Downloading and CD Burning among Teenage Online Consumers in the US, by Age, 2003 (as a % of respondents)

	12-13	14-15	16-17	18-19	20-22	Average
If there were serious risk that I would go to jail or have to pay a fine for downloading, I would stop*	69%	64%	74%	61%	68%	68%
If it took twice as long to download music, I would stop*	33%	28%	28%	29%	31%	30%
I buy fewer CDs because I can download any song I want	23%	25%	31%	37%	37%	30%

Note: *those who download
Source: Forrester Research, June 2003

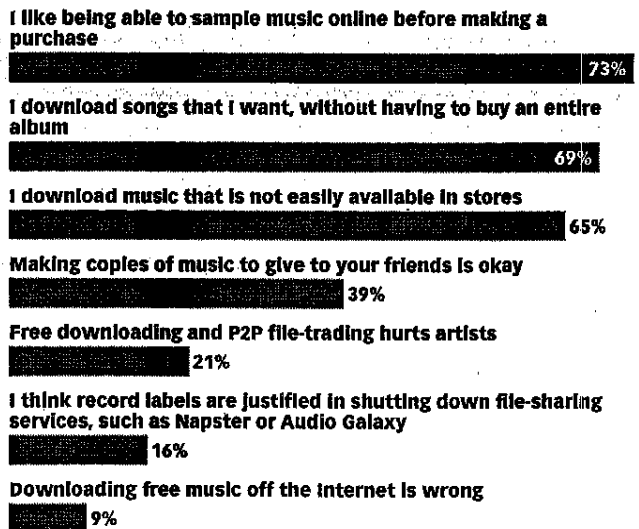
050920 ©2003 eMarketer, Inc.

www.eMarketer.com

Online music services have bet that they can compete with essentially free services by offering some of their benefits over physical distribution. These benefits include song sampling (although Buy.com, Amazon.com, and now more physical stores offer samples of songs on CDs) and inexpensive single tracks. While singles are available on CDs, they are relatively expensive. According to Ipsos-Reid, offering free samples and individual songs for sale are popular consumer features. However, Apple has reported that approximately half of the songs sold via its iTunes music store have been sold as part of an album. While this may seem to contradict Ipsos-Reid's findings, the half that have been sold as singles still represent a huge proportion shift from the world of physical CDs.

Only 39% of Ipsos-Reid respondents considered making copies of giving copies of music to friends okay, which is an illuminating finding since sharing among friends is a behavior that has a long-established precedent in the physical world. While covered by the same copyright laws, it was the sharing among strangers that served at the heart of the original Napster's controversy. Only 9% those surveyed believed that downloading free music off the Internet was wrong, but the Ipsos-Reid survey preceded the RIAA consumer lawsuits.

Attitudes toward Downloading Music Online among Downloaders in the US, December 2002 (as a % of respondents who strongly/somewhat agree)



Note: n=740

Source: Ipsos-Reid, March 2003

048409 ©2003 eMarketer, Inc.

www.eMarketer.com

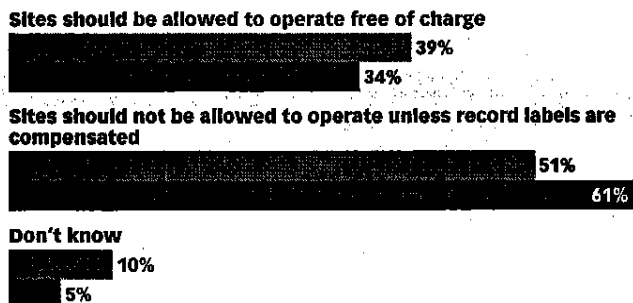
F. Consumer Attitudes

Regarding downloading music that is not easily accessible in stores, online music services have room to improve in meeting this demand. Music by independent and unsigned artists is difficult to find at any digital music retailer. The main online site for these artists – MP3.com – was shuttered after its acquisition by CNET Networks, although CNET promises to recreate the community and make legal free music available again through Download.com.

With Napster 2.0 currently boasting the largest music catalog at only half a million titles, online services are currently scrambling to add more popular artists and titles to their ranks. For example, in the iTunes music stores, many albums are incomplete, and some can be purchased only as individual tracks. The Beatles catalog, which was late to make the CD transition, is also absent from both the iTunes Music Store and Napster 2.0.

Sympathy for peer-to-peer services also seems to be declining slightly. When asked by Edison Media Research whether sites should be allowed to operate free of charge, fewer respondents agreed in 2003 than in 2002. But when a variation of that question regarding the necessity of record label compensation was asked, labels received greater support. 61% of consumers agreed in 2003 as opposed to 51% in 2002.

Attitudes of US Downloaders toward Music Downloading Web Sites, 2002 & 2003 (as a % of respondents)

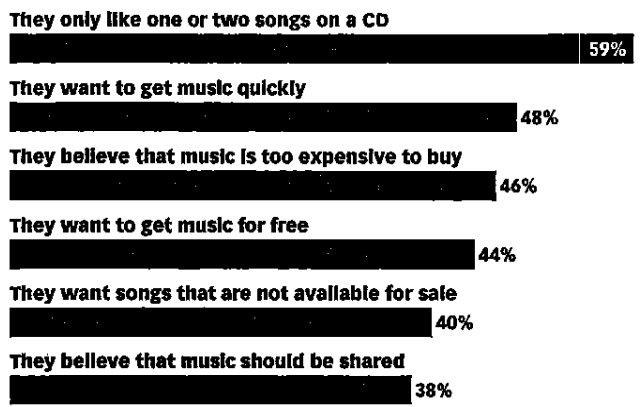


■ 2002 ■ 2003
 Source: Edison Media Research, June 2003
 052693 ©2003 eMarketer, Inc. www.eMarketer.com

The latest generation of music services has generally done a good job of addressing the stated preferences of teens, according to Harris Interactive. Harris found that the three leading reasons for downloading music without paying by teens were getting only a song or two from a CD, getting music quickly and saving money. Online services have provided a la carte song selection and can often offer files faster than peer-to-peer services that often require lengthy queues.

However, while digital albums often cost less than new physical CDs (especially after tax or shipping), older or less popular CDs can often be found used or at clearance for less than the \$9.95 that is the standard pricing for digital music services. They also come without any rights-management enforcement technology. eMarketer found that used CDs in good condition – a legal acquisition could be purchased online at Amazon.com and Half.com for \$2 less than their digital versions, even after a standard shipping surcharge of \$2.50 for Media Mail postage. Such purchases, however, certainly do not offer the instant gratification of a download.

Reasons that Teens* Download Music without Paying, 2003 (as a % of respondents)



Note: *among teens who have never paid to download music
 Source: Harris Interactive, October 2003
 052982 ©2003 eMarketer, Inc. www.eMarketer.com

F. Consumer Attitudes

Labels will need to keep an eye on profitability through digital services even if the wares of these stores thwart the endless copying cycle of unprotected CDs. Consumers are still attracted to the CD for reasons that may include the tangibility of a purchased product, its gift value, its compatibility with a broad range of playback devices and its artwork. E-Poll found that less expensive CDs were by far the most appealing option for consumers purchasing music, and several labels have made steps toward reducing the price of CDs. According to the RIAA, most of the cost of a CD is due to reimbursements that would need to take place in a digital world as well as the need to subsidize unsuccessful CDs – the vast majority – with profitable ones.

Most Appealing Music Purchasing Alternatives according to US Consumers, October 2003 (as a % of respondents)

Reducing CD prices by at least \$5

65.5%

Offer downloads at price per song

22.7%

Offer CD singles

11.8%

Note: n=1,162 ages 13+

Source: E-Poll, November 2003

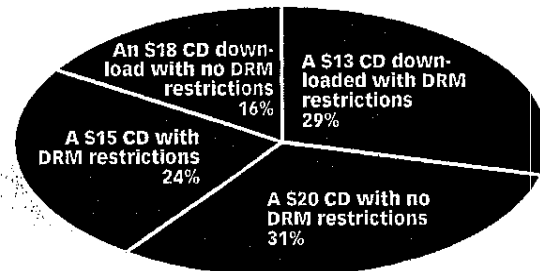
053465 ©2003 eMarketer, Inc.

www.eMarketer.com

Furthermore, data from Parks Associates shows that consumers continue to prefer, and claim a willingness to pay a premium for, CDs without digital rights management technologies. When presented with four options for obtaining music, more respondents in broadband-networked households (a relatively affluent sample) preferred a \$20 CD without DRM restrictions than a \$15 CD with DRM restrictions. However, when it came to downloads, respondents preferred a \$13 album download with DRM restrictions to an \$18 album download without restrictions. Even though the price difference of \$5 was the same for both forms of music, respondents were less price-sensitive toward CDs. Reasons for the contrast might include:

- The belief that downloaded music is easier to share and therefore DRM is more understandable
- Concerns about the compatibility of CDs with DRM with existing playback devices
- A psychological threshold of around \$14 where consumers accept DRM.

US Internet Users' Preferred Access to Purchased Music, 2003



Source: Parks Associates, December 2003

054531 ©2003 eMarketer, Inc.

www.eMarketer.com

Finally, to reap the benefits of a global music market in which approximately half of the revenue comes from outside of the US, online music services must expand beyond the borders of their home market. In December 2003, Nielsen//NetRatings found that European usage of KaZaA had outstripped US usage for the first time. While 9.35 million Europeans used the KaZaA application or visited the KaZaA sites from home in October, just 8.24 million US at home users did so in the same month. NetRatings attributed the shift to declining US usage in the wake of RIAA consumer lawsuits.

The RIAA may need to find an alternative to consumer lawsuits outside the US as well. Recent legislation in Canada has made it legal to download music from peer-to-peer sites within the provinces, although uploads are still illegal. Copyright holders would be compensated from taxes on sales of portable music players that rise with capacity. However, the low volume of these players and their easy availability from US retailers may not offset the losses particularly if the law encourages more consumers to download.

eMarketer View

Over one-third of US Internet users download music. By examining consensus data and recent adoption trends, eMarketer estimates that 34% of US Internet users have downloaded music in 2003. While adoption of new legal services is growing slowly, the threat of consumer lawsuits has more curtailed usage of peer-to-peer file sharing.

Online retailers will have the most success in selling digital music as a break-even product or loss leader. The mass appeal and low price of music make it an excellent impulse purchase, but few digital music stores today integrate sales of digital music with CDs or related products. Barring a restructuring of music industry cost structures, retailers will need to capture profit elsewhere given thin margins on digital music are untenable. Mass-market retailers such as Best Buy already use CDs as a loss leader; Online retailers such as Amazon.com, which will launch digital music alongside CD sales and its CDNow discount buyers' club, will reap the highest overall value from selling digital music.

Digital music retailers are meeting the most popular stated demands, but have much room to improve. Digital stores such as the iTunes Music Store, BuyMusic.com and Napster 2.0 offer several advantages over CDs, such as sampling, nearly instant access, and purchasing music by the song. They are still not as liberal as CDs in terms of rights management, but offer more flexibility than first-generation services. Their next great challenges are creating a greater selection of popular artists, increasing exposure of independent and unsigned artists and expanding into markets outside the US.

RIAA consumer lawsuits have had minimal impact on volume downloaders, but could have future benefits. The RIAA consumer lawsuits have been effective at shifting consumer attitudes regarding the legality or morality of file sharing, but have had a disproportionate impact on those who are least responsible for illegal downloads. However, the lawsuits may have short-term benefits in curtailing piracy among the next wave of broadband users and long-term benefits in affecting the attitudes of the younger music downloaders. To maintain their effect, on consumers' attitudes, the trade group will have to continue suing consumers.

Stores will emerge as the dominant acquisition model, but subscriptions may emerge as a viable and profitable niche market. Contrary to the protests of digital music service providers offering subscriptions, current pricing for digital music is not expensive, especially when compared to CDs. Furthermore, songs are unlikely to get less expensive given already thin margins and expenses inherent in music production, compensation and subsidization. Subscriptions contrast with how music has traditionally been acquired, but digital music may yet spawn new usage models. Satellite radio and MusicChoice (indirectly) have provided a precedent for consumers paying for music via subscription, much as cable provided a precedent for consumers paying a subscription for television.

Related Information & Links

Related Links

RIAA

<http://www.riaa.org/>

iTunes Music Store

<http://www.apple.com/itunes/store/>

KaZaA

<http://www.KaZaA.com/>

Limewire

<http://www.limewire.com/>

MusicMatch Downloads

http://www.musicmatch.com/download/music_intro.htm

Napster 2.0

<http://www.napster.com/>

BuyMusic.com

<http://www.buymusic.com/>

MusicNow

<http://www.musicnow.com/>

RealOne Rhapsody

<http://www.realone.com/>

MusicNet

<http://www.musicnet.com/>

Contact

eMarketer, Inc.
75 Broad Street
32nd floor
New York, NY 10004

Toll-Free: 877-378-2871
Outside the US: 212-763-6010
Fax: 212-763-6020
sales@emarketer.com

Spotlight Contributors

Yael Marmon	Director of Research
Krikor Daglian	Researcher
Tracy Tang	Researcher
David Berkowitz	Senior Editor
Kwanza Osajyefo Johnson	Data Entry Associate
Dana Hill	Production Artist

Data
August 2003

Viewpoint TechStrategy Research

August 2003

From Discs To Downloads

FORRESTER
RESEARCH
ANALYTICS
CONSULTING
CORPORATION

Helping Business Thrive On Technology Change





By Josh Bernoff

With Chris Charron

Ayanna Lorian

Charles Q. Strohm

Greg Flemming

Headquarters

Forrester Research, Inc.

400 Technology Square

Cambridge, MA 02139

USA

Tel: +1 617/613-6000

Fax: +1 617/613-5000

www.forrester.com

1983 FORRESTER 2003

The TechStrategy™ Report

AUGUST 2003

From Discs To Downloads

Hard media is in jeopardy; By 2008, revenues from CDs will be off 19%, while DVDs and tapes will drop 8%. Piracy and its cure -- streaming and paid downloads -- will drive people to connect to entertainment, not own it.

MARKET OVERVIEW

- 49% of 12- to 22-year olds downloaded music last month.
- Half of downloaders say they now buy fewer CDs.
- One in five young file sharers has downloaded a movie.

ANALYSIS

- File sharing has lopped \$700 million off of music sales.
- Proliferating on-demand media services will overtake piracy.
- In five years, 33% of music sales will come from downloads.
- CD sales will be down 30% from their 1999 peak.
- Various forms of video on-demand will gross \$4.2 billion.

WHAT IT MEANS

- Portals and cable win the on-demand media sweepstakes.

ACTION

- TV networks: Get those DVDs of popular series out quickly.

RELATED MATERIAL

- Online spreadsheet projecting online music and movie revenues and their effect on physical-media sales and rentals.

GRAPEVINE

ENDNOTES

© 2003 Forrester Research, Inc. All rights reserved. For more information, contact Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139, USA. Tel: +1 617/613-6000. Fax: +1 617/613-5000. www.forrester.com. For more information, contact Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139, USA. Tel: +1 617/613-6000. Fax: +1 617/613-5000. www.forrester.com. For more information, contact Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139, USA. Tel: +1 617/613-6000. Fax: +1 617/613-5000. www.forrester.com.

From Discs To Downloads
MARKET OVERVIEW

MARKET OVERVIEW

Downloaders Threaten Entertainment Sales

Two in 10 Americans engage in file sharing, and half of these admit to decreasing their CD buying. Worse, many of these same consumers have downloaded full-length movies. Downloaders think music labels and studios are incredibly greedy, but fear of prosecution would stop them.

ASSESSING THE EFFECTS OF FILE-SHARING YOUTH AND ADULTS

US CD sales are down 15% since 2000. Consumers' embrace of file-sharing technology like Kazaa and the encouraging start of paid services like Apple's iTunes beg the question: Will entertainment delivery on CDs and DVDs become obsolete? To find out, we examined all elements of the downloading and streaming phenomenon -- pirate and legitimate, music and video. Our data comes from three sources:

1. Forrester's June 2003 US Youth Online Study of 1,170 people age 12 to 22.
2. Forrester's Consumer Technographics® Q2 2003 North American Study of 4,782 adults 18 or older, a mail survey.
3. Peer-to-peer monitoring firm BigChampagne. For three years, BigChampagne has measured file-sharing activity by sampling online searches as well as the contents of shared directories on networks like Kazaa, Morpheus, and Lime Wire.

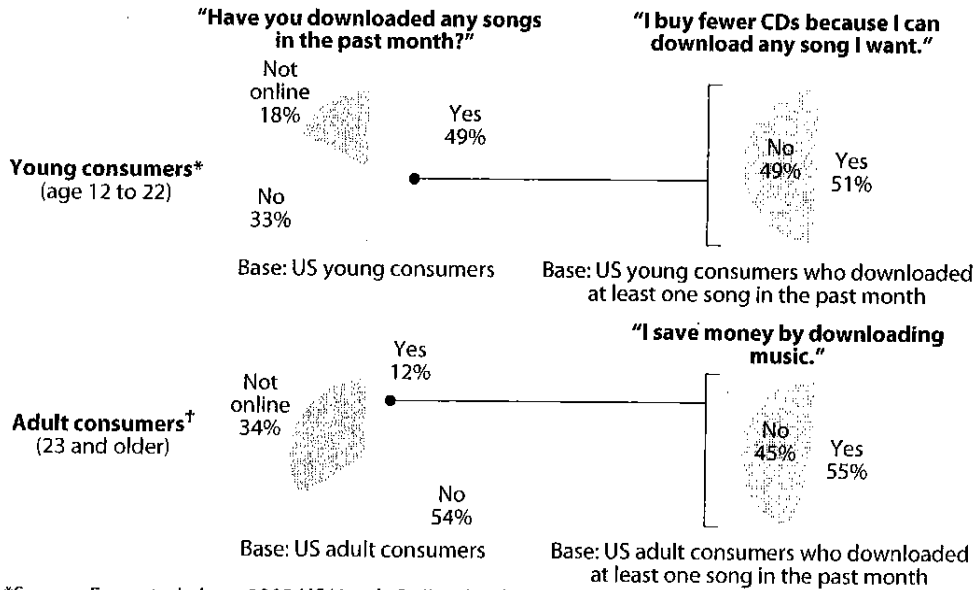
Two Consumer Segments Are Sinking The CD Business

One conclusion stands out from our consumer research: Not all downloaders are created equal. First off, young consumers (age 22 and younger) are far more likely to use file-sharing software -- half of them use it compared with only one in nine older consumers (see Figure 1). But regardless of age, about half of file sharers say that they now buy fewer CDs. Based on their age and attitudes toward downloading and CD buying, we divide entertainment consumers into six segments (see Figure 2).

- **The bad news: Juvenile Pirates and Retro Rippers substitute for CD buying.** Ten percent of US consumers admit to buying fewer CDs because they download. Those 22 and younger -- Juvenile Pirates -- downloaded 23 songs in the past month and burned 3.8 CDs. Their older counterparts -- Retro Rippers -- downloaded and burned slightly fewer. Together, they buy 13% of all CDs, a proportion that would be much higher if they didn't share files.

**From Discs To Downloads
MARKET OVERVIEW**

Figure 1 Downloading Is Far More Prevalent Among Young People



*Source: Forrester's June 2003 US Youth Online Study

†Source: Forrester's Consumer Technographics® Q2 2003 North American Study

Source: Forrester Research, Inc.

- The good news: Young Samplers and Burner/Buyers buy as they download.**
 Another 9% of consumers say that downloading hasn't affected their music buying. Half of youthful downloaders -- we call them Young Samplers -- are buying more than a CD a month, and two out of three of them say they'll buy the album from the song they just downloaded. Among older downloaders, the Burner/Buyers segment buys even more CDs than their young counterparts. These active CD buying segments account for 17% of all CDs sold in the US.
- The neutral news: Unwired Youth and Oblivious Adults don't download.**
 Half of Americans age 22 and younger and 88% of those 23 and older don't use file-sharing software. While these consumers represent 81% of Americans, they account for only 71% of CD buying.

From Discs To Downloads
MARKET OVERVIEW

Figure 2 Downloading And Buying Behavior By Segment

Segmenting consumers by downloading and buying behavior

	Download and decrease CD buying	Download and don't decrease CD buying	Don't download
Age 12 to 22*	Juvenile Pirates 5%	Young Samplers 5%	Unwired Youth 10%
Age 23 and older†	Retro Rippers 5%	Burner/Buyers 4%	Oblivious Adults 72%

Characteristics of consumer segments

Demographics	Age 12 to 22*			Age 23 and older†		
	Juvenile Pirates	Young Samplers	Unwired Youth	Retro Rippers	Burner/Buyers	Oblivious adults
Male	49%	57%	48%	57%	50%	50%
Average age	17	17	16	38	40	49
Have broadband	64%	58%	19%	42%	48%	14%
Online behavior‡						
Downloaded a full-length movie	23%	18%	0%	N/A	N/A	N/A
Have and use an MP3 player	30%	33%	15%	28%	21%	6%
Average CDs burned	3.9	2.5	0.7	3.7	3.1	0.4
Average songs downloaded	23	14	0	18	12	0
Burned most recent download onto a CD	42%	20%	0%	39%	26%	0%
Burned whole album for last download	10%	2%	0%	10%	9%	0%
Offline behavior						
CDs bought in the past 90 days	1.9	3.6	2.3	3.3	4.2	1.7
Likelihood to buy CD of most recent download	47%	67%	n/a	50%	58%	N/A
CDs in collection	88	91	63	176	180	81
Percent of all CD purchases	4%	8%	11%	8%	9%	60%
Attitudes						
"People should be able to download music for free"	79%	67%	46%	84%	60%	38%
"If there were serious risk of jail or a fine, I would stop downloading"	69%	64%	N/A	N/A	N/A	N/A

Base: US young consumers

Base: US adult consumers

*Source: Forrester's June 2003 US Youth Online Study

†Source: Forrester's Consumer Technographics Q2 2003 North American Study

‡In the past 30 days

Source: Forrester Research, Inc.

From Discs To Downloads
MARKET OVERVIEW

A Broad Swath Of Young Consumers Hates -- And Fears -- Music Companies

Many of the young consumers we surveyed responded to an open-ended question about their actions in their own words. Regardless of segment, they raged against the high cost of CDs and the perceived greed of music executives and artists, using these opinions to rationalize their behaviors. RIAA prosecution scares them; 68% of those who download said fear of jail or a fine would stop them, and their comments reflect those sentiments (see the July 16, 2003 Forrester Brief "Can Young File Sharers Be Stopped? Yes!"):¹

"I just recently stopped downloading music due to RIAA lawsuits. However, I have bought more CDs due to being able to download three to five songs and deciding to buy based on this selection of tracks." (Juvenile Pirate, male, 19)

"Musical artists and actors make way too much money. It's almost sickening. Then we, the little guys, download a bit of music or movies, and they make a million or two less a year and it's a big deal. If we're using these downloads for personal use, there shouldn't be a problem. They should leave us alone."

(Young Sampler, male, 13)

"The record companies are very unfair! They want people to pay \$18 for a CD when a blank CD only costs about \$0.99 . . . They are way overcharging. If they would fairly price CDs at maybe \$3 then people wouldn't want to download so much music and they would just buy the CD! RECORD COMPANIES ARE UNFAIR AND ARE PART OF THE SYSTEM, GO AGAINST THE SYSTEM!!!!!!!!!!!" (Young Sampler, female, 16)

"My folks don't want me downloading stuff. They told me why it's wrong, and I agree." (Unwired Youth, male, 14)

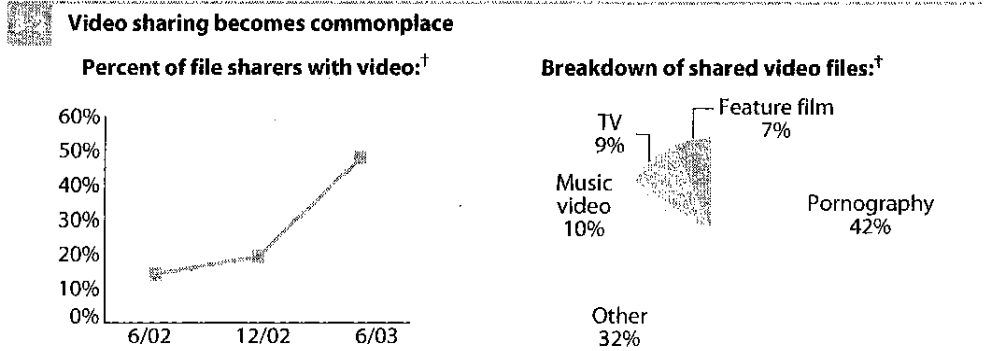
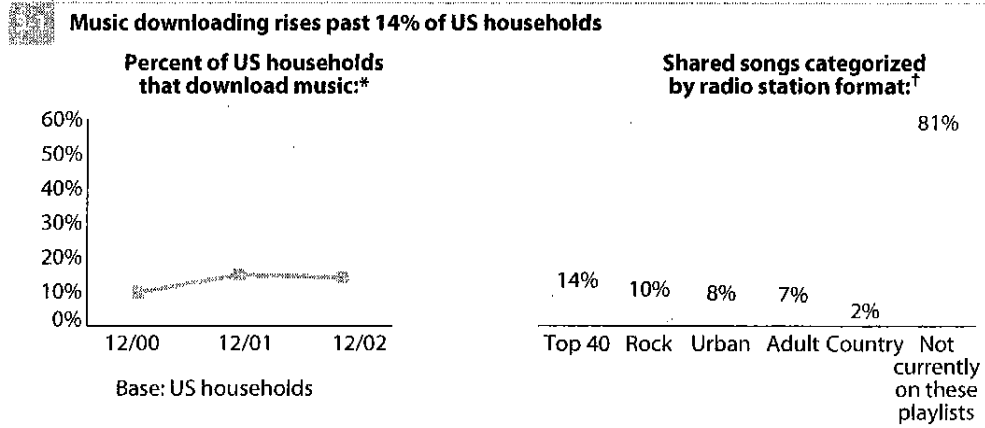
File Sharing Is On The Rise . . . For Both Music And Video

BigChampagne's historical monitoring of file-sharing activity and our youth survey both point to the same conclusion: Not only is file sharing up, but video makes up a larger portion of it (see Figure 3).²

- **Big sharers remain active.** As new users jumped onto file-sharing networks, the average shared-file directory observed by BigChampagne had 194 files in it this June -- down from 329 last June.³ Even so, in the past year, the proportion of file sharers with more than 400 files available has remained between 7% and 9%.
- **Video file sharing has become far more prevalent.** Of the active file sharers BigChampagne monitors, 48% share video files. And among heavy file sharers with more than 400 files, 70% had at least one video file. While many of the video files are short clips -- 42% were pornography, and 10% were music videos -- studios should note that 9% were TV shows and 7% were feature films.

From Discs To Downloads
MARKET OVERVIEW

Figure 3 Music Downloading And Video Sharing On The Rise



*Source: Forrester's Consumer Technographics 2001-2003 North America Benchmark Studies
 †Source: BigChampagne

Source: BigChampagne and Forrester Research, Inc.

- **Young consumers are beginning to share video.** One in five Juvenile Pirates and one in six Young Samplers report downloading a full-length movie in the past month. Juvenile Pirates are transferring their substitution behavior to video: 25% say DVDs are too expensive, and 11% say they now buy fewer DVDs.

From Discs To Downloads

ANALYSIS

ANALYSIS

The Slow Death Of The Disc

Broadband, widespread storage, and digital rights protection will make on-demand music and movie services possible. Music and movie companies will embrace them as the best defenses against piracy, shifting 33% of music sales and 19% of home video revenues to streaming and downloading.

Result: CDs and DVDs will go the way of the LP.

TECHNOLOGY-BASED THREATS NEED TECHNOLOGY SOLUTIONS

We were wrong. We used to think downloading wasn't responsible for the music industry's problems (see the August 2002 Forrester Report "Downloads Save The Music Business").⁴ But based on our most recent surveys, we now estimate that file sharing is responsible for almost \$700 million of the \$2 billion reduction in CD sales since 1999 (see Figure 4). And movie executives have escalated concerns about this to the highest management levels, fearing that file sharing will soon decimate their businesses as well.

Technology Megatrends Created This Problem -- And Can Solve It

How did we get to these crossroads? Broadband connections, cheap and widespread storage, and ubiquitous processing power have forever liberated media from physical objects like CDs, tapes, and DVDs. But the same technology forces that brought entertainment companies to this crisis point contain the promise of media's salvation -- the ability to create media services that consumers will pay for.

- **Ubiquitous bandwidth enables commerce, not just file sharing.** By the end of next year, 30 million consumers in the US will be spending \$14 billion annually on broadband connections. These are the target customers who will pay MusicMatch to program their custom radio stations or Movielink to deliver a high-quality film in an hour, far faster than the random speed of connections on Morpheus.
- **Cheap, widespread storage allows home media management.** Media-laden PC hard drives are just the beginning -- now add a \$300 iPod that holds "2,500 Songs In Your Pocket" or an Internet-connected TiVo with 80 hours of video. But as storage spreads media throughout the home, it becomes a hassle to move entertainment to the right place. Vendors like Apple or Digeo will succeed by taming and organizing it for easy access and effortless enjoyment anywhere.

From Discs To Downloads
ANALYSIS

Figure 4 Do The Math: Almost \$700 Million Lost To Downloading

Segments that decrease CD buying due to downloading			
	Juvenile Pirates	Retro Rippers	Total
Number of consumers	11 million	12 million	23 million
Annual number of CDs bought by these consumers	30 million	57 million	87 million
Estimated % increase if they did not download*	x 84%	27%	x 47%
Additional CDs they would buy if not affected by downloading	25 million	16 million	41 million
Average cost per CD (US\$)	x \$17.00	\$17.00	x \$17.00
Revenues lost to music industry due to downloading	\$425 million	\$272 million	= \$697 million

*Note: Estimate based on behavior of corresponding segments (Young Samplers and Burner/Buyers) who download but do not decrease CD purchasing.

Source: Forrester Research, Inc.

- **Affordable processors put rights management in sight.** What enabled Rio MP3 players to cost less than \$150 and MPEG-enabled cable boxes to lease for \$5 per month? The rapid spread of low-cost media processing chips. Now PC OS vendors are tying these devices together with technology like Apple's Fairplay and Microsoft's Windows Media DRM. The result is a vision promoted passionately by Microsoft's CTO, Craig Mundie: files that can be copied easily but won't play unless tokens on the device prove the user has the right to use them.

HOW ENTERTAINMENT COMPANIES WILL GET THEIR GROOVE BACK

Based on our conversations with content companies and industry organizations, we believe the entertainment industry will succeed in its efforts to use legitimate downloading and streaming services to restore growth. In contrast to two years ago, we didn't find a single executive stuck on the idea of "defending the status quo" of selling physical objects. Instead, media companies are attacking the problem by creating what we call on-demand media services:

Services that offer consumers instant access to a wide selection of media content, paid for by subscription or by the piece.

On-demand media services have the potential to turn pirate losses into gains, even as they break the disc-based shackles that now hold back entertainment. To succeed with on-demand media services, entertainment companies will need to: 1) slow online piracy through technical and legal action, and 2) support the creation of on-demand alternatives.

From Discs To Downloads**ANALYSIS****Entertainment Companies Will Make File Sharing Unpleasant And Risky**

Music labels and film studios know they can't stop file sharing any more than state troopers can stop speeding. But right now, consumers trade files without worry, care, or guilt. Entertainment companies can slow piracy with legal and technical deterrence.

- **Lawsuits and publicity make file sharing scary.** Lawsuits against the likes of Kazaa parent Sharman Networks could take years to resolve, but the Recording Industry Association of America (RIAA) has hit on a winning strategy in suing individuals. As our survey reveals, more than two out of three young downloaders say they'd stop if there were a serious risk of jail or a fine. The key is continuing the drumbeat of publicity, including articles about the RIAA's subpoenas and the Justice Department's prosecution of a man for posting "The Hulk" on Kazaa.
- **Technical interference makes downloading unproductive.** Entertainment companies hire vendors like Overpeer and MediaDefender to create "spoofed" decoy files for songs and movies. Seventeen percent of online young consumers have downloaded a spoofed file. While young users with lots of time can just go back and download another copy of the file, busier consumers may just give up -- especially if reasonably priced, legitimate alternatives exist. And spending hours to download a movie, only to find that it's a fake, will seriously slow video trading.
- **Universities are trying to make file sharing impossible.** Led by Penn State President Graham Spanier, universities are requesting bids on technologies to block file trading, which now fills more than half of the bandwidth used at many schools. And institutions like Boston College warn incoming freshmen that the administration will hand over the names of pirates if labels ask for them.

Competing On-Demand Music Services Will Soon Proliferate

Last year, we said music services needed three elements to meet the "Consumer Bill of Rights" -- broad selection, flexible payment terms, and music that supports CD burning and copying to portables. Apple's iTunes Music Store, the first commercial service to meet those criteria, sold 5 million downloads in its first six weeks. Here's what's coming:

- **2003 to 2004: Varied Windows services prove that downloads work.** In the next nine months, at least 10 Windows-based music services will emerge (see Figure 5). AOL already has 90,000 MusicNet subscribers. MusicMatch and RealOne Rhapsody will differentiate with their media players and Web radio; BuyMusic will try to leverage its early entry with personalized recommendations from ChoiceStream. By the end of 2004, Apple and possibly MusicMatch will emerge as leaders, file sharing will be in decline, and downloads and on-demand subscriptions will bring in \$270 million (see Figure 6).

From Discs To Downloads
ANALYSIS

Figure 5 On-Demand Music And Movie Services

Music services	Differentiator	Selection*	Price to burn		DRM/file format	Prospects
			Per month	Per track		
Apple iTunes Music Store	Easy interface and integration with iPods	5 majors, indies, 300K tracks	None	\$0.99	Apple aac	☆☆☆ Year-end Windows launch enters crowded field
AOL MusicNet	Leverages AOL user base	5 majors, indies, 400K tracks	\$8.95	TBA	Real	☆☆ Taps AOL Music traffic to gain share
BuyMusic	First viable non-subscription Windows service	5 majors, indies, 300K tracks	None	\$0.79 to \$1.19	Windows Media	☆☆ Choicestream recommendations will help
MusicMatch	Organizes tunes; creates impulse buys from radio	3 majors, indies	None	TBA	Windows Media	☆☆ 130,000 radio subs could expand niche
RealOne Rhapsody	Leverages RealOne audience	5 majors, indies, 325K tracks	\$9.95	\$0.79	Real or Windows Media	☆☆ Success depends on RealOne portal subscribers
Roxio Napster 2.0	Napster name, CD burning competency	500K tracks planned	None	TBA	Windows Media	☆☆ By Christmas launch, won't stand out
Echo	Backing and cross-promotion from retailers	TBA	Not likely	TBA	TBA	☆ Must prove it can launch
eMusic	Eclectic selection, MP3 format	1 major, indies, 225K tracks	\$9.95	Free	MP3, no DRM	☆ Majors won't support MP3 format
FullAudio MusicNow	Programmed radio stations	5 majors, indies, 200K tracks	\$9.95	\$0.99	Windows Media	☆ Despite partnerships, lacks differentiation
Liquid	Circuit City, Tower, FYE partnerships	300K tracks	None	\$0.99	Windows Media or Liquid	☆ Where will Wal-Mart take it?
Movie services	Delivery method	Selection†	\$ per month	\$ per rental	Target device	Prospects
iN DEMAND	Cable VOD	6 majors, indies, 200+ movies	None	\$3.99	Digital cable box	☆☆☆ Right customers, delivery to TV set
Movielink	Internet	6 majors, indies, 400 movies	None	\$3.99	PC	☆☆ Studio support, but needs PC/TV connections
CinemaNow	Internet	3 majors, indies, 200+ movies	None	\$3.99	PC	☆☆ Studios could support Movielink competitor
MovieBeam	TV spectrum	Only Disney so far, 100 movies	TBA	TBA	Special set-top box	☆☆ Obstacles: monthly fee, special set-top box

☆☆☆ Likely winner ☆☆☆ Contender ☆ Don't bet on it

*Major labels are Sony, BMG, Warner, EMI, and Universal. Indies are independent labels.

†Major studios are Sony, Warner, Fox, Disney, Paramount, Universal, and MGM. Indies are independent studios.

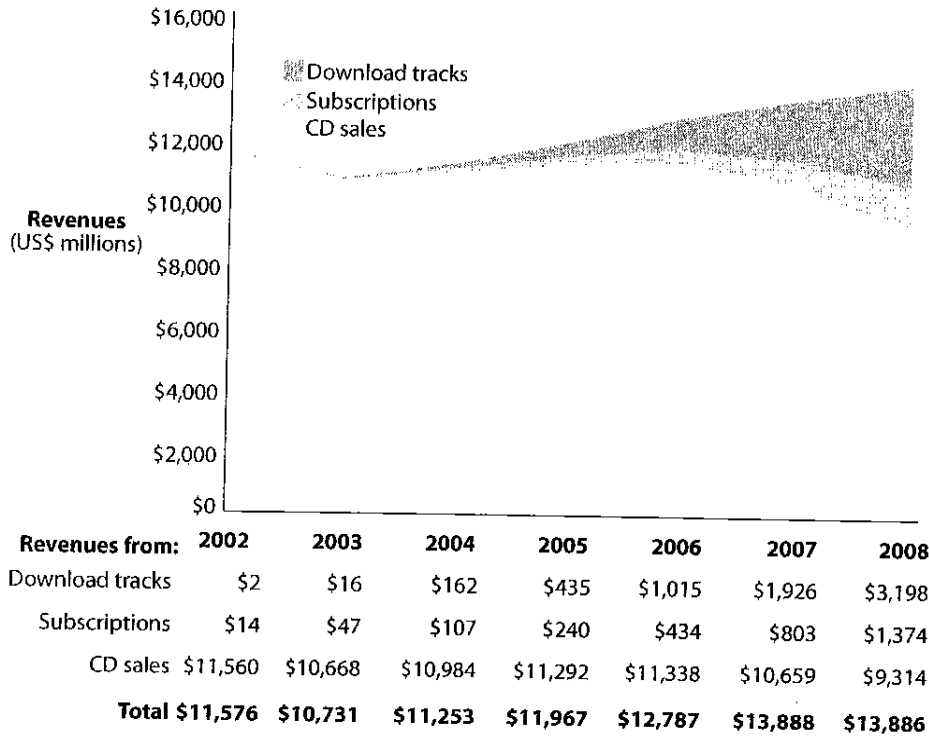
Note: "Movies" includes only recent releases.

Source: Forrester Research, Inc.

**From Discs To Downloads
ANALYSIS**

Figure 6 Forecast: US Music Revenues, 2002 To 2008

The spreadsheet detailing this forecast is available by clicking the online "Get Data" button above this figure.



Source: Forrester Research, Inc.

- 2005 to 2006: Music sales grow again as subscription services take off.**
 By 2005, music buyers will recognize that: 1) buying music à la carte makes for costly collections, and 2) everything you want will be available online. As consumers get more comfortable with online music, subscription services like RealOnc Rhapsody and AOL MusicNet will overshadow à la carte services like Apple iTunes. Three years from now, subscriptions and downloads will account for \$1.4 billion in a revitalized \$12.8 billion music industry. CD sales, while buoyed by the marginalization of piracy, will remain 15% below the industry's peak in 1999.
- 2007 and 2008: CDs become passé.** By 2008, 33% of music sales will come from downloads. Online downloads will come with extensive artwork, extras like musician interviews and alternate versions, and lifetime service -- none of which discs can match. Portables, hard-drive-enabled set-top boxes, and computers will

From Discs To Downloads ANALYSIS

ship with a tens of thousands of songs preloaded; consumers will unlock them by signing up for a subscription. Artist royalties will be paid based on SoundScan reports compiled from samples of consumers' most recent playlists. Like LPs, discs will show up at yard sales. Label profits will rise as the expense of manufacturing, shipping, and returns on plastic discs fades away.

Successful Movies On-Demand Will Steal Business From Home Video

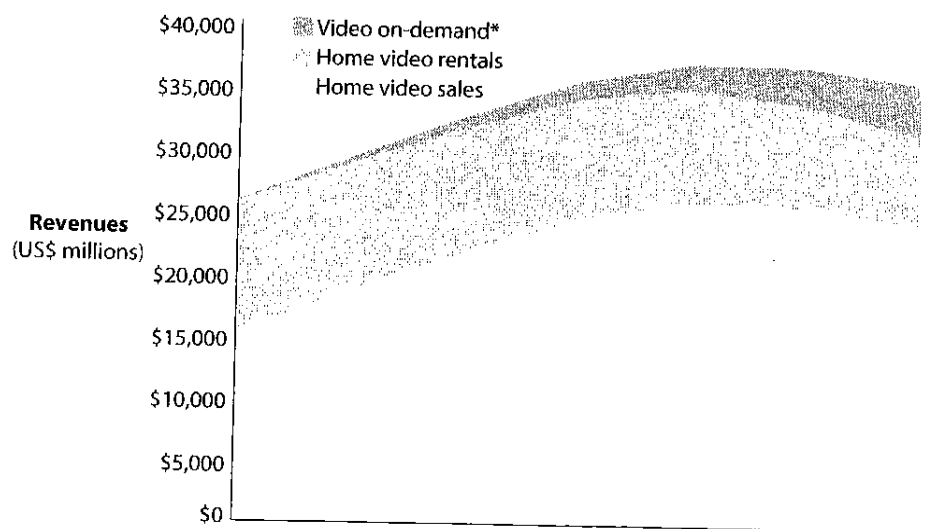
Piracy in movies is three years behind what's happening in music. While 11% of young people online have downloaded a movie, only 5% report that they buy fewer DVDs as a result. But rather than risk the meltdown that happened in music, studios are responding by embracing all forms of on-demand delivery. Here's what will happen:

- **2003 to 2004: Cable on-demand breaks through, but other channels lag.** In the next two years, 22 million US households will have access to movies through video on-demand (VOD) (see the November 2002 Forrester Report "Will Ad-Skipping Kill Television?").⁵ As these consumers become familiar with the benefits of VOD -- vast selection, no trip to the store, no late fee -- rental rates for movies on-demand will float past one per month, rivaling video rental rates. On-demand movies will appear on the same day as rental discs, removing any time advantage for hard media. VOD revenues of around \$900 million will climb to represent a respectable 3% of the home video market (see Figure 7).
- **2005 to 2006: Home networking and satellite kick in.** In the next three years, cable VOD and other on-demand distribution options will reduce store-based movie rental revenues by 16%. Satellite will imitate cable-style VOD with networked PVR set-top boxes. Analog cable customers with cable modems will get free wireless Internet adapters that stream movies to the TV set. The end result of all this activity? By 2006, one in three households will have video on-demand movies. Studios, finding VOD more profitable than shipping discs, will advance the VOD windows to within two months of theatrical release.
- **2007 to 2008: Movie sales, not just rentals, go virtual.** Five years from now, all the extras now available on DVD will be duplicated on cable and Internet VOD. Even as DVD-player penetration surpasses 70%, leading-edge consumers will be wondering if it's worth it to upgrade to a high-definition DVD player. Home video rental revenues at Blockbuster and Wal-Mart will drop 37%, leaving these stores to focus on sales. But cable and satellite will begin to nibble away at DVD sales by allowing permanent downloads of content to PC and PVR hard drives.

From Discs To Downloads
ANALYSIS

Figure 7 Forecast: US Video Revenues, 2002 To 2008

The spreadsheet detailing this forecast is available by clicking the online "Get Data" button above this figure.



Revenues from:	2002	2003	2004	2005	2006	2007	2008
Video on-demand*	\$86	\$410	\$904	\$1,412	\$2,041	\$2,984	\$4,162
Home video rentals	\$10,383	\$10,201	\$9,925	\$9,530	\$9,005	\$8,122	\$7,091
Home video sales	\$15,322	\$18,709	\$21,795	\$24,589	\$26,045	\$25,834	\$24,556
Total	\$25,791	\$29,320	\$32,418	\$35,531	\$37,091	\$36,940	\$35,809

*Cable, Internet, and other VOD

Source: Forrester Research, Inc.

From Discs To Downloads
WHAT IT MEANS



WHAT IT MEANS

By 2008, US CD sales will be down 30% from their 1999 peak. Disc- and tape-based home video, having peaked in 2006, will be off 10%. AOL's 2003 decision to sell off its manufacturing plants will look prescient. Meanwhile, the race for dominance in on-demand media services will generate winners and losers.



Big winners: Internet portals.

Portals will tap their established subscribers, interface expertise, and delivery infrastructure to lead in on-demand media services. AOL will make MusicNet and MovieLink the linchpins of its AOL for Broadband offering. MSN will drive traffic with links from within the Windows Media Player. Yahoo! needs alliances with BuyMusic, Napster, or CinemaNow to compete. Without the traffic the big boys have, scrappy RealNetworks will need to build a unique niche offering from its 1 million streaming content subscribers, Listen.com music service, and exclusive streaming media content.



Winners: cable and telcos.

Broadband suppliers would much rather sell on-demand media than deal with bandwidth-hogging, subpoena-generating music pirates. Broadband leader Comcast will become a kingmaker -- a bundling partnership with Roxio Napster or MusicMatch could instantly vault those companies ahead. Time Warner will deliver music and video to both the TVs and PCs of its Road Runner customers. Using services like RealOne Rhapsody, telcos like Verizon will deliver music to DSL-enabled PCs, wireless PDAs, and mobile phones.



Winners: artists and directors.

With the overhead of disc manufacturing and the bottleneck of physical distribution removed, artists at all levels will benefit. Popular evergreen artists like Madonna, U2, and Bruce Springsteen will release a treasure-trove of concert and studio material, mining the archives and selling 100-track packs -- the download equivalent of boxed sets -- for \$50 of pure profit. At the other end of the spectrum, unsigned bands will tap vendors like Rockslide and concert promoters like Clear Channel to package performances into downloads, generating extra cash as Phish does at livephish.com. Independent filmmakers will put content on CinemaNow or post their own sites, soliciting "download donations," to fund their next effort.

From Discs To Downloads
WHAT IT MEANS



Winners and losers: device makers.

While on-demand media services will create opportunities for all sorts of new devices, as HP recently demonstrated, they'll also erode the market for traditional CD and DVD players. And hardware makers' leverage in the content space will be limited. Apple should expand its music service to include video, boosting sales for its Cinema HD Display. D&M Holdings, parent of Rio and ReplayTV, will have to partner with video and music aggregators to supply its device stable. Sony's attempts to supply media to PlayStations will fall victim to game-console interface challenges.



Losers: media conglomerates.

Media giants will be stymied as others take over their customer relationships. News Corp. will be able to retain some clout by partnering with telcos to turn its DIRECTV boxes into streaming media portals. But Disney's MovieBeam won't attract enough consumers to provide much leverage, leaving The Mouse to elbow for space on cable VOD interfaces. EMI, Bertelsmann, and whoever ends up with Universal will settle for promoting bands and wholesaling content to portals and broadband companies.



Big losers: retailers.

Disc-centered media stores like Tower Records and Blockbuster will close by the hundreds as volume and selection of CDs and DVDs shrink. They will sell or rent their brands to other competitors, creating services with names like "Blockbuster Movielink" and "Virgin MusicNow." Diversified media retailers like Wal-Mart, Circuit City, and Best Buy will survive by shifting CD and DVD floor space to expand media device sales. Only online-focused media sellers like Amazon.com and Netflix have a chance to build niche portals for media mavens.



And the ultimate winners: consumers.

The consumer benefits of on-demand media services reach far beyond getting media when you want it. Unlocked from the straitjacket of a physical package, on-demand media will include feedback and community as standard features, allowing consumers to vote and chat with fellow consumers of the same content. Interactivity will blur the lines between games and content, as all video and audio develops interactive elements and rich media pervades gaming applications.

From Discs To Downloads

ACTION

ACTION



Radio companies should promote online portals.

Impulse purchases -- I hear, I want, I buy -- will make the download business work. Radio companies like Clear Channel should commerce-enable their Net radio stations, working with vendors like BuyMusic on one-click buys of any song that catches your ear. With technologies from Digital Innovations and Audible Magic, portable players will be able to recognize any song a user hears -- on car radios, TV sets, at a friend's house -- and mark it for purchase when the user reconnects to his PC or Mac.



Television companies have three years to get those DVDs out.

This moment in media is unique -- DVD players are becoming ubiquitous, but VOD content remains sparse. In the next three years, TV studios like Warner and Fox should crank out DVDs of popular series like "E.R.," "Seinfeld," and "Boston Public." By 2006, the focus of negotiations will shift to terms for making content available on cable and Internet "basic VOD" tiers (see the June 5, 2003 Forrester Brief "How 'Windowing' Can Unleash Video On-Demand").⁶



Advertisers should extend sponsorships online.

Sponsoring entertainment -- as Coors did for Kid Rock, and BMW did for James Bond -- gives advertisers a conduit to consumers in an era where do-not-call lists, spam filters, and TiVo threaten ad impressions. Online, these relationships can go further. Apple can subsidize downloads of tracks by 50 Cent, who fondles an iPod in his latest video. And when Will Smith's next action movie comes out from Warner or DreamWorks, each VOD stream, Internet trailer, or MovieBeam rental should feature a 10-second spot from Nike, Cingular Wireless, or the US Army -- whoever will pay the most.



Movie studios need Internet distribution to go around cable.

Cable will continue to push VOD, but movies on-demand must compete for attention with HBO on Demand and hundreds of free on-demand shows. To refocus cable operators' attention -- and keep their share of revenues high -- studios like MGM and Universal should build up competing on-demand channels. They should entice satellite operators to build broadband Internet connections into set-top boxes, enabling Internet satellite streaming and downloads. Disney should license its MovieBeam functionality for TiVo boxes, so they can download movies on-demand from TV broadcast bandwidth.

From Discs To Downloads
RELATED MATERIAL

RELATED MATERIAL

Online Resource

To see the underlying spreadsheet detailing the forecast in Figures 6 and 7, click on the "Get Data" button above each figure.

Methodology

This report includes the results of Forrester's June 2003 US Youth Online Study, an online survey of 1,170 young people between the ages of 12 and 22. We also include results from Forrester's Consumer Technographics® Q2 2003 North American Study of 4,782 adults 18 and older; we only cite results in this report from adults age 23 or older. Finally, we gratefully acknowledge the contribution of data published here from BigChampagne, a research company that for the past three years has monitored file-sharing activity by using proprietary technology to measure search requests and the contents of shared directories on peer-to-peer networks starting with Napster, and including Kazaa, Morpheus, and Lime Wire.

Individuals Interviewed For This Report

We interviewed prominent individuals in the file-sharing and downloading debate, including Russell Frackman, lead counsel for many of the RIAA's content lawsuits; James Miller, assistant professor of Economics at Smith College and author of *Game Theory At Work*; Cary Sherman, president of the Recording Industry Association of America; and Graham Spanier, president of Pennsylvania State University and co-chair of the Joint Committee of the Higher Education and Entertainment Communities.

From Discs To Downloads
RELATED MATERIAL



Companies Interviewed For This Report

Adobe <i>www.adobe.com</i>	Electronic Freedom Foundation <i>www.eff.org</i>	Motion Picture Association <i>www.mpa.org</i>
Altnet <i>www.altnet.com</i>	EMI <i>www.emigroup.com</i>	Movielink <i>www.movielink.com</i>
AOL <i>www.aol.com</i>	FullAudio <i>www.fullaudio.com</i>	MusicMatch <i>www.musicmatch.com</i>
Apple <i>www.apple.com</i>	Get Digital <i>www.get-digital.net</i>	MusicNet <i>www.musicnet.com</i>
Audible Magic <i>www.audiblemagic.com</i>	Gracenote <i>www.gracenote.com</i>	The News Corporation <i>www.newscorp.com</i>
BayTSP.com <i>www.baytsp.com</i>	Grokster <i>www.grokster.com</i>	Overpeer <i>www.overpeer.com</i>
BigChampagne <i>www.bigchampagne.com</i>	iN DEMAND <i>www.indemand.com</i>	Pennsylvania State University <i>www.psu.edu</i>
BuyMusic.com <i>www.BuyMusic.com</i>	Lime Wire <i>www.limewire.com</i>	RealNetworks <i>www.real.com</i>
CinemaNow <i>www.CinemaNow.com</i>	Listen.com <i>www.listen.com</i>	Recording Industry Association of America <i>www.riaa.org</i>
CNET Networks <i>www.cnet.com</i>	Loudeye <i>www.loudeye.com</i>	Roxio <i>www.roxio.com</i>
Digital Networks North America <i>www.rioaudio.com</i>	MediaDefender <i>www.mediadefender.com</i>	Universal Music Group <i>www.umusic.com</i>
Disney <i>www.disney.com</i>	Microsoft <i>www.microsoft.com</i>	Warner Bros. Entertainment <i>www.warnerbros.com</i>
Echo <i>www.echo.com</i>	Mitchell, Silberburg, & Knupp, LLP <i>www.msk.com</i>	Warner Music Group <i>www.wmg.com</i>

Related Research

July 16, 2003 Forrester Brief "Can Young File Sharers Be Stopped? Yes!"
 May 12, 2003 Forrester Brief "Downloads: 13% Of Europe's Music Market In 2007"
 May 2003 Forrester Report "Who Will Network The Home?"
 April 29, 2003 Forrester Brief "Apple Breaks The Digital Music Logjam"
 March 4, 2003 Forrester Brief "Highlight: Downloading Beats Streaming Hands Down"
 January 20, 2003 Forrester Brief "Downloading Music Hurts Europe's CD Sales"
 December 9, 2002 Forrester Brief "My View: Digital Denial"
 November 15, 2002 Forrester Brief "EMI, pressplay, And MusicNet Rev Up Online Music"
 November 2002 Forrester Report "Will Ad-Skipping Kill Television?"
 September 25, 2002 Forrester Brief "Europe: 2 Billion Music Downloads Per Year"
 August 2002 Forrester Report "Downloads Save The Music Business"
 March 2001 Forrester Report "Movie Distribution's New Era"

From Discs To Downloads
GRAPEVINE

GRAPEVINE

Yes, but what do young consumers *really* think?

We couldn't resist including a few more typical comments from our youth survey, simply because young people are so passionate about music and downloading.

"Artists rip us off. They stick one good song on and then a bunch of junk." Male, 15

"Burning CDs is wrong but charging \$20 for a CD is wrong also." Female, 16

"I always like to test-drive things. You wouldn't eat food you haven't sampled so why are they so hard on the downloaded stuff?" Female, 17

"All my friends download movies and CDs but my mom says it is no different than stealing it from the store because people get cheated out of their money." Male, 12

"My parents just bought a computer that you can burn CDs on, but for some reason I feel it is kind of wrong, it makes me feel like I am stealing." Female, 15

"[Downloaders] should be prosecuted as thieves and be given fines and jail terms. Theft is still theft whether it is electronic or with a weapon." Female, 16


"Some people download 50 songs a week, and Apple has the nerve to charge \$0.99 per song? That's \$50 a week! People don't spend that much on CDs!" Female, 20

Would you rather be loved or feared?

The MPAA has initiated a big campaign to show how downloading hurts the little people who make movies (see www.respectcopyrights.org). The basic pitch: "If you loved us, you wouldn't hurt us like this." Meanwhile, the RIAA publicizes its subpoenas to strike fear into the hearts of file sharers. Which is more likely to work? Fear. Based on the responses we heard, consumers have no love (and therefore no guilt) to spare for entertainment companies, artists, or actors. But fear is effective. The rub, though, is this: what action do you take when the pirate is an innocent-looking 10-year-old?

We're shocked, *shocked*, to find out that copyrighted software is being shared.

We nearly fell off our chair when Greg Bidson, CTO and COO of Lime Wire, told us he found it "shocking" that consumers use his product to post copyrighted software files. A software vendor must need a pretty finely tuned moral compass to build a program that makes it easy to share music, and then get offended when people use it to share code.

From Discs To Downloads**ENDNOTES**
ENDNOTES

- 1 Consumers share more and more up to age 20, but all age groups are equally afraid of prosecution.
- 2 BigChampagne's data accurately reflects the state of file sharing at any given moment, but because the most active file-sharing users are more likely to be online, BigChampagne's results over-represent this active group.
- 3 BigChampagne monitors all files in shared directories, including audio files, video files, and other file formats.
- 4 Last year, we surveyed only consumers 18 and older and were unable to detect the decrease in CD buying based on consumers' self-reported CD purchases in the 90-day periods before and after the survey.
- 5 Unlike personal video recorders, video on-demand can preserve advertising values. Networks and cable operators will embrace video on-demand to create revenue from on-demand TV consumers.
- 6 To get shows into basic video on-demand, cable operators should adopt windows -- time-limited availability for programs. This preserves some degree of appointment viewing and will be far more acceptable to owners of those programs.

STUDY JUSTIFICATION

As a security solutions provider, Palisade Systems has always been aware of significant risks associated with peer-to-peer (P2P) file sharing applications. When file-sharing applications first became available, music and movie files were the most common files shared and bandwidth usage the most important issue.

This study was proposed to analyze the content P2P users were searching for and to show that P2P applications are being used to share files that create legal liability issues.

EXECUTIVE SUMMARY

March 20, 2003
Peer-to-Peer Study Results

Porn Tops File Sharing Usage

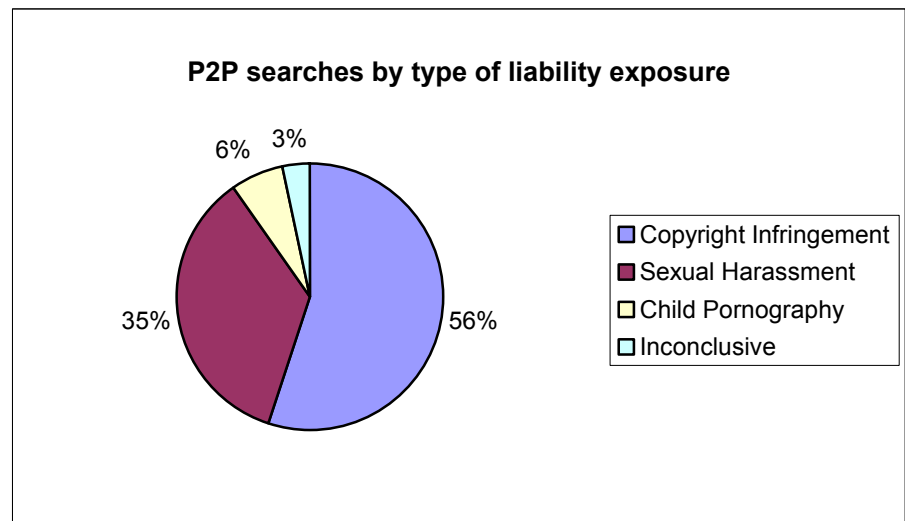
The peer-to-peer (P2P) study conducted by Palisade Systems shows that file-sharing applications have no legitimate value in the workplace. Since the emergence of Napster in 2000, file-sharing applications have become more sophisticated. The Gnutella file-sharing applications, such as Morpheus, LimeWire, and BearShare, make it possible to trade virtually any file on a user's computer where the P2P software resides.

Palisade Systems monitored a file-sharing network for nearly three weeks and discovered:

- 42% of all requests were for adult or child pornography
- 38% of all requests were for copyrighted audio files.

Overall, 97% of all activities on a P2P network could result in a criminal or civil suit against a business for copyright infringement, sexual harassment, or felony-level offenses.

Organizations allowing P2P activity to operate unchecked on their networks are vulnerable to substantial security risks as well as civil and criminal legal liability. Better and more secure methods are available for sharing files in the workplace environment without the liability and security dangers inherent in P2P file sharing.



To discuss the results of this study, please contact:

Stephen Brown, Product Marketing Manager
Palisade Systems, Inc., 2625 North Loop Drive, Suite 2120, Ames, IA, 50010
Tel: 888.824.0720
E-mail: sbrown@palisadesys.com

BACKGROUND ON PEER-TO-PEER FILE-SHARING APPLICATIONS

RISKS ASSOCIATED WITH P2P FILE-SHARING APPLICATIONS

Introduction to P2P

P2P applications reside on individual computers that can communicate directly with other computers running similar software on a network. Once a connection is established, the P2P application makes it possible to share virtually any file between the connected machines.

Napster emerged as the first of many P2P applications (such as KaZaA, Morpheus, WinMX, and Xolox) that have gained popularity over the past two years for free access to music and movies on the Web.

How P2P Networks Work

To understand the risks associated with P2P, it is important to understand how they work.

P2P networks are made up of individual machines running similar software that communicate directly over the Internet. A machine that connects to this network is not only connecting to one other machine, but to a web of connected machines that are linked to each other by one common thread—the P2P application. Once connected, the P2P application allows information to be exchanged freely among the participants. Because there isn't a central hub of communication but instead many decentralized points of communication, P2P activities are difficult to detect and stop. This opens up organizations to the many risks inherent in P2P applications.

P2P Risks

Though well documented in the general and technical press, many people do not adequately appreciate the scope and severity of risks that are posed by the use of P2P applications.

Liability Risks

Civil or criminal liability issues could arise from 97% of the files requested on a P2P network. (See P2P Liability Exposure Graph.)

The following is a quote from attorney Daniel Langin, whose practice has specialized in information security and business liability for over 13 years, regarding the legal exposures to businesses from unregulated file sharing:

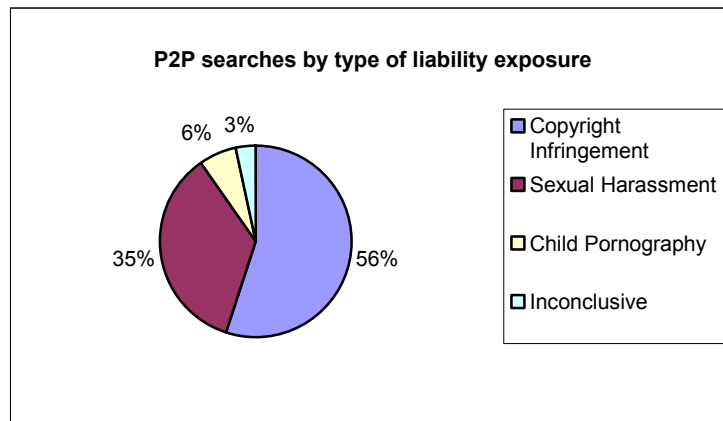
“Significant potential liability risks may stem from the use of peer-to-peer functionality. The most obvious risk is that of a civil suit for copyright infringement. Late last year, the Recording Industry Association of America (RIAA) sent a form letter to Fortune 1000 companies putting them on notice of potential liability stemming from employee use of P2P. The damages and legal fees involved in such cases can be significant.

P2P poses additional risks. The amount of sexually explicit materials traded over peer-to-peer may also open up an organization to discrimination suits as a hostile workplace. Especially dangerous is P2P use associated with child pornography, which exposes individuals to a felony-level offense.”ⁱⁱ

In addition to corporate liability issues, there are also serious personal criminal liabilities facing users illegally downloading and sharing copyrighted materials. In a recent CNet article, DeClan McCullagh explained felony charges that may be brought against an individual using P2P file sharing applications.

“An obscure law called the No Electronic Theft (NET) Act that former U.S. President Bill Clinton signed in 1997 makes peer-to-peer (P2P) pirates liable for \$250,000 in fines and subject to prison terms of up to three years. The NET Act works in two ways: In general, violations are punishable by one year in prison, if the total value of the files exceeds \$1,000, or, if the value tops \$2,500, not more than five years in prison. Also, if someone logs on to a file-trading network and shares even one MP3 file without permission in “expectation” that others will do the same, full criminal penalties kick in automatically.”ⁱⁱ

Copyright infringement through the illegal sharing of copyrighted video and audio files is the greatest risk facing organizations and is classified as a federal felony through the Digital Millennium Copyright Act (DMCA). Downloading legal pornographic video and images, if it takes place in the work environment, may constitute grounds for a sexual harassment lawsuit. Felony charges can apply to downloading child pornography, which represented 6% of all activity. Downloads where liability is inconclusive accounted for only 3% of all searches.



Security Risks

In addition to criminal and civil liability risks, there are several network security risks associated with P2P.

- **Accidental sharing of sensitive files** – Confidential business and personal files may be shared with other P2P users. Unknowingly the user grants access to multiple folders or the entire hard drive containing these files.
- **Releasing viruses and trojans** – Files are most often from unknown users. Music files or executable program files exchanged on a peer-to-peer network can contain viruses or trojans. The files can circumvent most email or Web download anti-virus solutions and the viruses are discovered after damage has been done.
- **Installation of spyware** – Applications such as KaZaA and BearShare require users to install spyware on their computer as a part of the licensing agreement. Spyware tracks the activities of the user and reports them to a third-party organization.
- **Bandwidth clogging** – A few users downloading movies or large files can easily clog an organization’s network halting business critical operations on the network.

The study focuses on quantifying the liability issues of P2P.

STUDY PROCEDURE

Palisade Systems acted as a node on a Gnutella network and gathered searches from February 6–23, 2003. During that time 22 million search results were collected in a database. Any information identifying the individual such as the Internet Protocol (IP) address were removed to maintain privacy of the users. In addition, none of the requested files were downloaded.

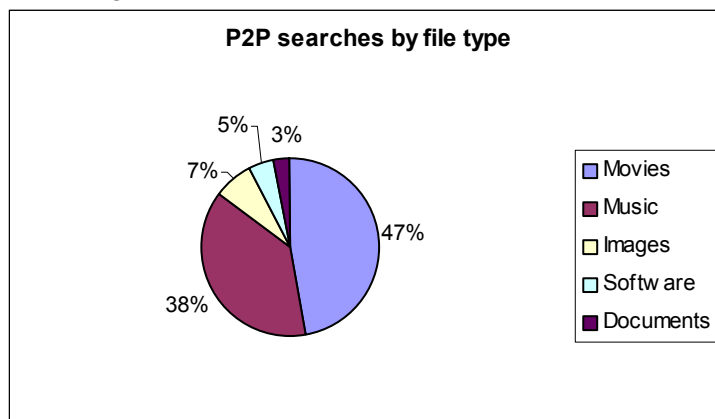
From these results, 400,000 were randomly selected for analysis. The database was queried using more than 654 keywords to determine the content of the searches. The searches fell into the following categories:

- **Audio files**
 - Legal – Files that can be traded legally through peer-to-peer networks either with permission of the artist or belonging to the public domain.
 - Copyrighted – Files that are traded without permission of the artist and therefore infringe on the copyright.
- **Video Files**
 - Copyrighted – Files that are traded without permission of the artist and therefore infringe on the copyright.
 - Pornographic – Files containing nudity and/or sexual content of adults.
 - Child Pornography – Files containing nudity or sexual content involving minors. (Note: This was treated as a separate category as possession of child pornography constitutes a felony.)
- **Image Files**
 - Legal – Files that can be traded legally with the consent of the artist or as public domain.
 - Pornographic – Files containing nudity and/or sexual content of adults.
 - Child Pornography – Files containing nudity or sexual content involving minors. (Note: This was treated as a separate category as possession of child pornography constitutes a felony.)
- **Software**
 - Legal – Software that can be traded legally through peer-to-peer networks either as freeware, with permission of the company, or as public domain.
 - Copyrighted – Files that are traded without permission of the software developer and therefore infringe on the copyright.
- **Documents**

STUDY RESULTS

Overall Content

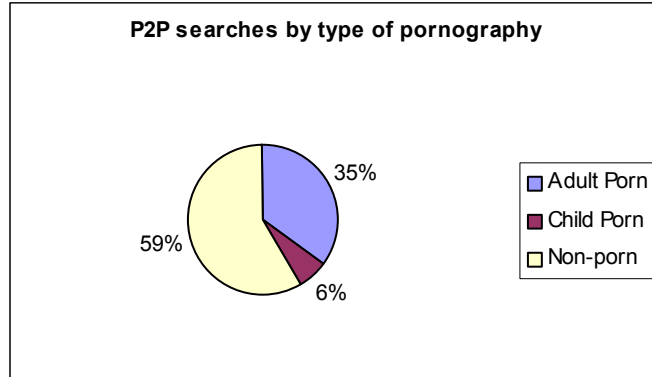
The majority of searches were for video, which were fueled by requests for pornography. Music files were 38% of requests. Searches for images represented 7% of overall requests, and software accounted for 5%. Legitimate or legal use of P2P file sharing constituted 3% of all searches.



Accessing Pornography

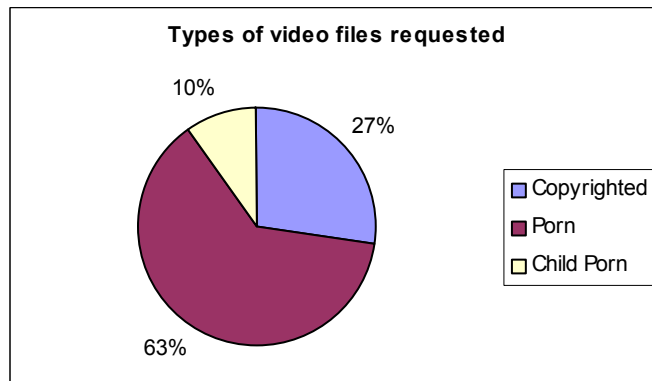
A strong reason for using P2P file sharing appears to be the easy access to pornography. Overall searches for pornographic materials accounted for 42% of all searches. This compared to nearly 38% of all searches for movies.

General pornography was the dominant search request with 35%. Child pornography, considered a separate category in the study due to its illegal nature, represented 6% of all search requests.



Video Files

The majority of video searches were for pornography. 10% of video searches were for child pornography. This compares to 27% of video searches for copyrighted movies.



Audio Files

Of the audio files requested, 99% were copyrighted, and 1% were legal audio files. In this study 150,000 songs were identified as being copyrighted material, compared to 1680 audio files that were legal to share.

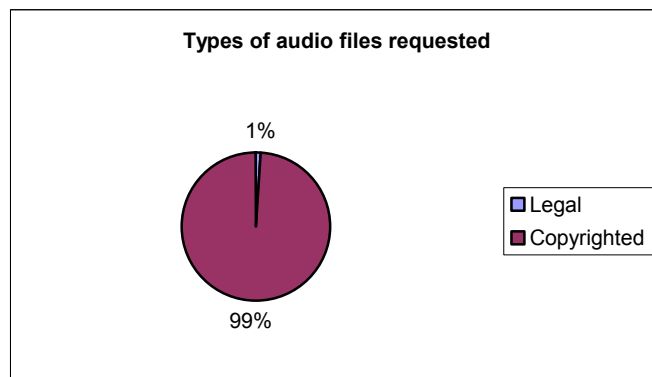
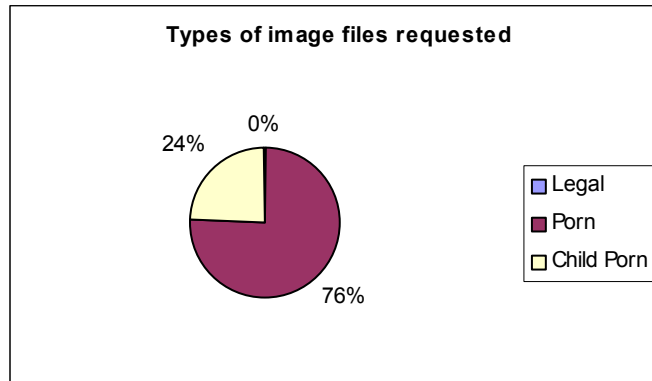


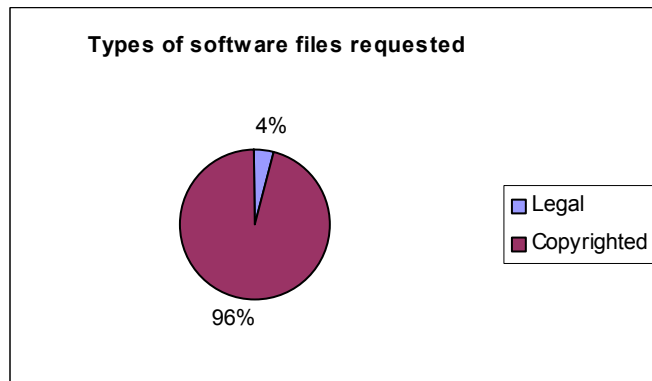
Image Files

Child pornography tends to be noticeably more prominent among image files accounting for over 24% of all searches for images. 75% of the images were pornography involving adults. Legal images accounted for less than 1% of the image files requested.



Software Programs

Overall software program files were 5% of the total files requested. Copyrighted programs were nearly 96% of all the software files requested. The most popular programs sought in searches included Macromedia Dreamweaver, Adobe PhotoShop, and Norton Antivirus, and Electronic Art (EA) The Sims. Legally traded software over peer-to-peer networks accounted for 4% of total software requests. These files include freeware and public domain software titles.



To discuss the results of this study, please contact:

Stephen Brown, Product Marketing Manager
Palisade Systems, Inc., 2625 North Loop Drive, Suite 2120, Ames, IA, 50010
Tel: 888.824.0720
E-mail: sbrown@palisadesys.com

ⁱ Quote is from an interview with Daniel Langin conducted by Palisade Systems on March 13, 2003. It was conducted after Mr. Langin reviewed the results of the survey.

ⁱⁱ DeClan McCullagh. "Perspective: The new jailbird jingle. CNet News.com. January 27, 2003.
Source: <http://news.com.com/2102-1701-982121.html>

P2P Fear and Loathing: Operational Hazards of File Trading Networks

John Hale, Nicholas Davis, James Arrowood and Gavin Manes

Center for Information Security, University of Tulsa

Abstract—Peer-to-peer (P2P) networking technology has revolutionized file sharing over the Internet. Proprietary and open source P2P ventures alike have taken flight, facilitating public file sharing on an unprecedented level. Unfortunately, careful investigation of P2P security and digital rights management issues has not followed hand-in-hand with wide-spread acceptance and use of the technology. P2P networking clients expose systems to a variety of security and privacy hazards. Moreover, rampant copyright infringement over P2P networks has spurred the development of electronic countermeasures to thwart would-be infringers. This paper examines the security and privacy risks associated with P2P networks, as well as electronic countermeasures to copyright infringement over P2P networks.

Index Terms— blocking, digital rights management, electronic countermeasures, file sharing, interdiction, network security, peer-to-peer networks, redirection, spoofing, viruses, worms.

I. INTRODUCTION

Peer-to-peer (P2P) networking technology has revolutionized file sharing over the Internet [2, 3, 4, 7]. Proprietary and open source P2P ventures alike have taken flight, facilitating public file sharing on an unprecedented level. Unfortunately, investigation of P2P security and digital rights management issues has not followed hand-in-hand with wide-spread acceptance and use of the technology.

P2P networking clients expose systems to a variety of security and privacy hazards. Systems running P2P networking clients may be vulnerable to software design and implementation flaws that provide an open door for hackers. What distinguishes this threat from that posed by flaws in other applications is that the heightened connectivity of systems running P2P clients greatly increases the level of exposure, and accordingly the risk of operation. Privacy concerns related to the potential for (and in some cases documented existence of) spyware embedded in P2P clients also have not diminished.

Moreover, the most popular P2P networks have become a breeding ground for copyright violations of all digital media – copyrighted music, movies, software and games are openly traded. Where cryptography has failed to provide a solution,

rampant copyright infringement over P2P networks has spurred the development of alternative electronic countermeasures to thwart would-be infringers. This paper examines security and privacy risks associated with P2P networks, as well as electronic countermeasures to copyright infringement over P2P networks.

II. PEER-TO-PEER TRADING NETWORKS

File sharing networks based on peer-to-peer technology typically embrace one of two server models; centralized or decentralized. The difference to users is transparent, but can have subtle implications for system security and for electronic countermeasures. This section briefly describes each model.

A. Centralized P2P Model

Napster popularized the centralized P2P model, and demonstrated the viability and power of a simple network overlay architecture on the Internet [2]. The Napster P2P model relies on a centralized server (or a collection of servers) to maintain an index of downloadable files on participating network clients (Figure 1).

To participate in this kind of a P2P network, a user must download and launch a software client. The client registers itself in the network by communicating to the server and listing the files available for download, which are located in a designated shared folder. The client also sends connection information to the server; its IP address, purported connection type (e.g., T3, T1, Cable, DSL or dial-up), and other metadata. Clients periodically send updates to the server to ensure a current index.

Keyword-based queries (Figure 1 - Q) for files are issued from a client to the server, which then reports back to the requesting client any hits (Figure 1 - H), identifying the location of all clients that have files matching the search criteria. A download request is then made from the originating client directly to the client hosting a desired file, and the download process begins (Figure 1 - D). Commonly, the download process is accomplished via a separate network protocol, e.g., HTTP – the protocol used to download web pages from sites across the Internet.

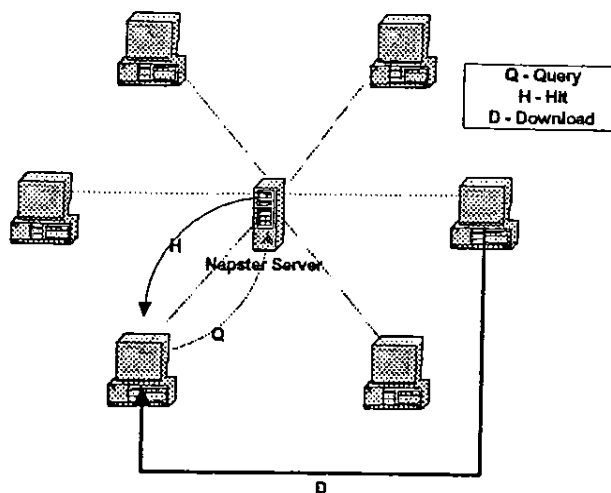


Figure 1: Centralized P2P Model.

The primary performance issue in the centralized model is that the server, since it must index every host and respond to every query, is a potential bottleneck. However, server replication is a simple and effective strategy for overcoming this obstacle, allowing P2P networks to scale in number of participating hosts. The tradeoff for this scheme is added complexity of server-to-server communication and logic for index integrity and consistency.

B. Decentralized P2P Model

The decentralized architecture features a purer implementation of the peer-to-peer networking philosophy (Figure 2). Gnutella and other decentralized P2P schemes rely on each client to support query/response functionality [3]. The only server-like systems involved in these networks are those nodes that help clients bootstrap themselves into the network by providing them with a list of peer node IP addresses in the client's neighborhood.

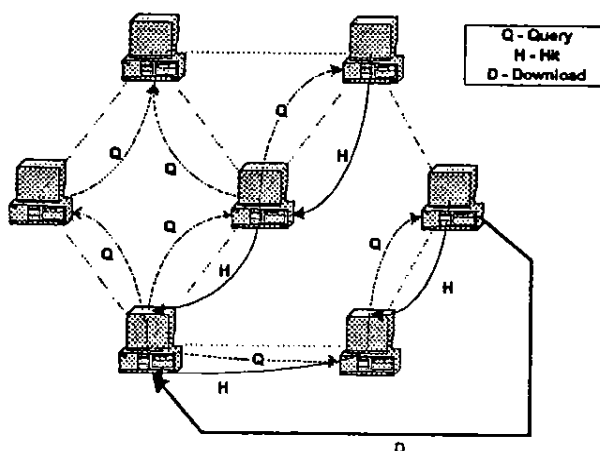


Figure 2: Decentralized P2P Model.

Once again, participation requires the installation of client software to launch the bootstrap process and issue and respond to queries. The collection of network nodes visible to a given client defines its horizon. The horizon for a node is dynamic and is directly related to timely network replies compared against Time-To-Live (TTL) parameters, which establish the lifetime (typically by hops) of query messages originating from a client.

In decentralized P2P networks, file queries (Figure 2 - Q) are issued from a client directly to other nodes in the client's horizon. Clients receiving queries may respond directly with a hit message (Figure 1 - H), or pass the query along to other nodes in its horizon. One subtle feature in the most common decentralized model implementation is that hit response messages traverse back through the original query path, as opposed to flowing 'directly' back to the query host from the responder. Download requests are made from the querying client directly to the client reporting the hit. (Figure 1 - D). Again, it is common practice for the actual download process to occur via a separate network protocol, such as HTTP.

III. P2P NETWORK THREATS

Most P2P networks share characteristics that increase the risk of operation for participating systems. Extreme and anonymous connectivity inherent in P2P networks creates an environment in which establishing and maintaining core security properties of integrity and non-repudiation is a difficult, if not impossible, task. P2P file traders run a higher risk of machine crashes, loss of privacy, even having their systems commandeered by hackers. Threats to P2P users may not only come from hackers lurking in dark corners of the network, but also from the client software itself. This section examines the dangers posed to P2P networks by spyware, trojan horses, system exploits, denial of service attacks, and worms and viruses.

A. Spyware

The most prevalent threat to user privacy in P2P networks is spyware. Spyware takes many forms; from annoying software that sends registration form data to third parties for consumer profiling, to more insidious programs that track user activity and steal sensitive information off of hard drives.

Developers routinely bundle spyware and adware with P2P clients as a way to generate a revenue stream from their freely downloadable software. In P2P networks, spyware complements adware by monitoring user behavior and constructing user profiles from various data sources on a user's system. In particular, P2P spyware tracks user browsing habits to facilitate target-marketing campaigns that often incorporate adware (pop-up and banner advertisements). In addition, registration data is regularly sold to direct marketing firms.

While there is no indication that this practice will diminish, "clean" versions of P2P clients (purportedly without spyware) have surfaced [5]. Even so, no foolproof method of checking for the absence of spyware in these (or any other) applications exists.

B. Trojan Horses

Trojan horses are executable code embedded in system or application software with unexpected and possibly malicious behavior. They may leak information, corrupt files, or allow an intruder to gain unfettered access to a system. The wide install base and lax security of personal computers running P2P clients makes them attractive targets for trojan horses.

However, the primary threat comes not from the core client itself, but from the collection of software and adware bundled with the client. In January 2002, Symantec classified a P2P client spyware program called "W32.DIDER" as a trojan horse because, even after users opted to block installation of the carrier code, it installed itself on users' systems [1]. The offending code was bundled in clients for four separate P2P networks. At the time, one of the P2P networks involved boasted a client install base of over 1.3 million systems.

C. System Exploits

System exploits take advantage of application-level vulnerabilities due to flaws in software. Exploits are often captured in scripts and posted on hacker websites that any novice can access. They can be designed to achieve a number of malicious objectives.

By far, the most common form of software system exploit is the buffer overflow attack. Buffer overflows capitalize on weak bounds checking of parameters to overwrite strategic regions of memory. In some cases, overflowing a parameter or variable may have no discernable effect. On the other hand, it may crash a system. In a skilled buffer overflow attack, executable code is written into memory and run, potentially giving a hacker full control over a host. Other kinds of system exploits, such as race conditions and trust abuse occur less frequently, but can yield similar results.

As in any program, P2P client software is susceptible to design and implementation flaws. Unfortunately, the open nature of P2P clients makes buffer overflow and other system exploits more likely, and potentially more devastating. P2P clients must, by definition, expose network service interfaces and other functions that can easily be probed for flaws and weaknesses by hackers. For example, an alleged cross-site scripting vulnerability was reportedly found in some early Gnutella clients and is currently under review [6]. The weakness allows attackers to execute arbitrary code on remote systems. Unfortunately, the increasing richness of P2P client service features and functions correspondingly increases the potential number of latent software vulnerabilities, which can lay dormant for years until they are discovered by a hacker.

D. Denial of Service Attacks

Denial of Service (DoS) attacks are among the most potent weapons in a hacker's arsenal. They are also the most challenging to contend with. DoS attacks can happen at any level of a network and/or application. Some DoS attacks may consist of malformed packets designed to crash systems. Others may rely on network traffic floods to take down a system or router, even engaging multiple hosts to force-multiply the impact of the attack; the most extreme of these enslave a legion of hosts in order to launch a massive wave of

packets at a target in a Distributed Denial of Service (DDoS) attack. Such attacks can encumber substantial collateral damage; while the intended target may be a host, an entire network could be equally impacted.

In as much as DoS attacks degrade performance or disrupt service for networks and systems, they likewise impact P2P users and networks. However, it is possible that certain types of DoS attacks may target hosts, or even specific applications on hosts, leaving other system elements relatively unharmed. For example, jamming the upload queue of a P2P client with a flood of download requests may effectively block other users from accessing files on that host, but have no other substantial impact on the host itself or the network to which it is connected.

E. Worms and Viruses

Worms and viruses have as much potential to overwhelm computers and networks as do DoS attacks. Both infect hosts via system exploit and/or social engineering, cover their tracks, and reproduce to move across a network. Worms propagate without human intervention, using network services and communication channels to spread. Viruses rely on humans to move from system to system. The payload in viruses and worms may be malicious or benign, but in either case the massive reproduction of self-replicating code may be enough to cripple hosts or regions of a network.

A recent spate of virus attacks has inflicted damage on popular P2P networks [8]. One of the earliest, the "Benjamin" virus, propagates itself across the Kazaa P2P network through a combination of social engineering and localized replication in share folders. The virus relies on a user download to move from machine to machine across the Internet. Once the code is activated, the virus copies itself to a shared directory under a variety of names and displays a website containing banner advertisements.

Even though these P2P viruses need humans to download them to spread, it is not difficult to envision a true P2P worm that replicates itself throughout shared folders by using vulnerable client communication channels. Such a worm might infect a host by identifying and exploiting a latent buffer overflow exposure residing in client network service functions. Copying its own code into the communication buffer, it would not rely on human interaction to propagate, and therefore could spread much faster.

IV. P2P DIGITAL RIGHTS MANAGEMENT

As researchers seek elusive cryptographic solutions to the digital rights management problem, a collection of electronic countermeasures have been developed that strike at digital piracy distribution models. Blocking, interdiction, spoofing and redirection all aim to inhibit the trading of copyrighted media in P2P file sharing environments. It is important to note the schemes described in this section do not engage "hacking" techniques to foil digital media piracy. Each technique has its relative merits and disadvantages, but collectively, they represent the only practical technological means of dealing with copyright infringement over P2P networks.

A. Blocking

The most straightforward technique for inhibiting illegal file trading in P2P environments is to block queries and/or hit response messages as they try to move across a network (Figure 3). This can be accomplished with a simple firewall or router by blocking the appropriate ports used by communicating P2P clients. The net effect of this approach is that regions of P2P networks are isolated from the rest of the network, unable to communicate or trade files. Successful implementation of this strategy requires control of some region of the network, and thus is ideally suited for enterprises and Internet Service Providers (ISPs). (While blocking helps some private enterprises cut down on digital piracy and curb bandwidth consumption, public ISPs appear more than reluctant to adopt this approach.) Depending on the implementation, a blocking solution may restrict P2P communications for an entire enterprise network, a subnet or collection of subnets, or an individual host.

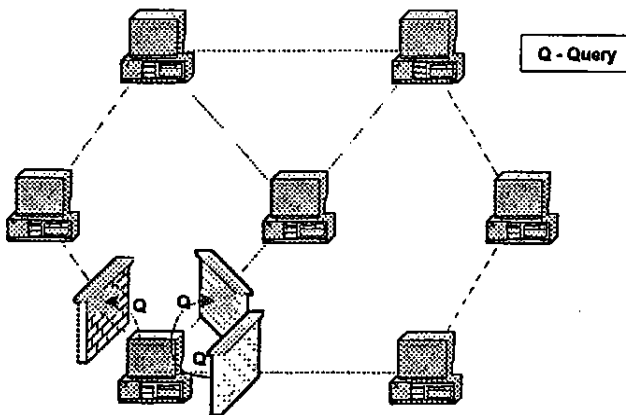


Figure 3: Blocking.

The drawbacks to this approach are significant. Blocking solutions typically cannot discriminate between illegal file trading and legitimate queries and downloads. Moreover, depending on the load of the network, the blocking hardware, the countermeasure may constitute a bottleneck. Lastly, simple port-hopping and tunneling strategies are effective ways to elude network blocking and filtering devices, making it more difficult to locate and disrupt copyright infringing downloads and communications.

B. Interdiction

Interdiction constitutes a high-level Denial of Service attack on P2P client download functions (Figure 4). The objective of this countermeasure is to swamp the download request queue of a copyright infringer with requests so that no illegal copyrighted media can be downloaded from the infringer's system by third parties. Implementation engages an array of hosts – interdiction servers – dedicated to locating infringers and issuing a stream of download requests to keep their queues filled over time.

This approach differs from low-level DoS attacks in that it surgically strikes at an application-level weakness – the limited capacity of the P2P client download request queue. Whereas a

conventional DoS flooding attack may direct thousands of messages at a target instantaneously, a slow but steady stream of download requests will likely suffice to greatly diminish an infringer's ability to share files over a P2P network. The principal drawback of this approach is that requests for legitimate media to the infringer's host are affected as well. In addition, smart clients may be programmed to ignore repeated download attempts from the same client in an attempt to circumvent the countermeasure.

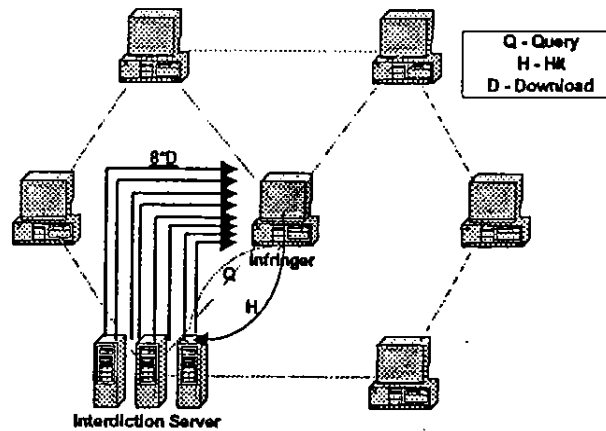


Figure 4: Interdiction.

C. Spoofing

Like interdiction, spoofing countermeasures aim to prevent digital media copyright infringement by overwhelming P2P networks (Figure 5). However, while interdiction attacks the download process, spoofing targets the search process. This technique floods P2P indexes with decoy metadata in a centralized architecture, e.g., Napster networks, and responds to queries for copyrighted media with bogus responses in a decentralized architecture, e.g., Gnutella networks. The intended effect of spoofing is to make locating authentic files in a trading network nearly impossible by ensuring that decoy hits drastically outnumber legitimate ones.

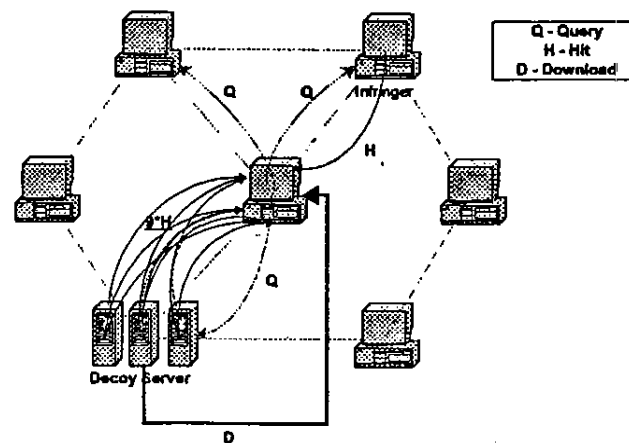


Figure 5: Spoofing.

Spoofing typically requires an array of systems serving up decoy information. The bandwidth economics of spoofing is more attractive than interdiction because the process yields a flood of media metadata, substantially less expensive than the constant stream of downloads incurred by queue jamming. Moreover, spoofing does not inhibit legitimate file trading by anyone, it targets the media, not the infringer.

Decoy media manufacture and download strategies play a key role in the success of spoofing schemes. Decoy media must appear authentic in all ways to requesting clients – in size, name, format, and all other media characteristics visible to users in P2P search engines. The download process can be metered to preserve network bandwidth. Download preview functions also pose a challenge to manufacturing decoys, but techniques have been proposed to construct decoy media files that appear authentic in their initial seconds of play. This minimizes the effectiveness of preview functions as decoy filters.

D. Redirection

Redirection perpetrates a bait and switch on users looking for copyrighted digital media in file trading networks (Figure 6). In Gnutella-style networks it exploits the messaging protocol, which mandates that the response path follow the query path for media searches. Intermediate hosts along the query path falsify and corrupt response messages (Figure 6 – H1) so that subsequent download requests (Figure 6 – D5) are misdirected. Strictly speaking, redirection in Napster networks is not possible without penetrating the server index core services.

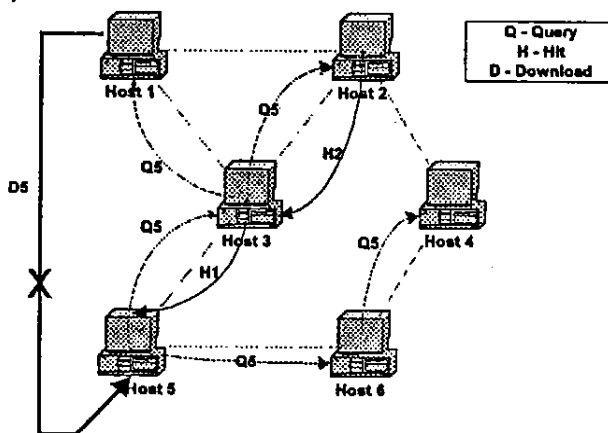


Figure 6: Redirection.

This approach has an ultimate effect similar to that of spoofing, except that its “decoys” actually replace some infringer search results. Would-be infringers even can be redirected to alternative content. However, a simple modification to the P2P messaging protocol permitting direct query responses (as opposed to responses that follow the query path) would eliminate the opportunity for intervening clients to alter or forge response messages.

V. CONCLUSIONS

Users and adopters of peer-to-peer technology must understand associated operational hazards, including inherent security vulnerabilities and exposures, as well as implications of imminent P2P digital rights management strategies. Next generation P2P networks promise greater anonymity, more powerful search engines, and anticipate an underlying Internet infrastructure that delivers broadband connectivity to virtually every desktop. Unless security architectures and electronic countermeasures for network media piracy keep pace with P2P technology, developers, network administrators and users alike will find increasing operational risk and greater digital media copyright protection challenges in the future.

REFERENCES

- [1] Borland, J., *File Sharing Programs Contain Trojan Horse*, Tech News – Cnet.com, <http://www.cnet.com>, January 2, 2002.
- [2] Dr. Scholl (pseudonym), *OpenNap Napster Protocol*, <http://opennap.sourceforge.net>, 2000.
- [3] LimeGroup, LLC. *The Gnutella Protocol Specification v0.4.*, <http://www9.limewire.com>.
- [4] Cho, S., *Understanding Peer-to-Peer Networking and File-Sharing*, <http://www.limewire.com/>, 2002.
- [5] Menta, R., *Clean LimeWire - All the flavor without all the SpyWare*, MP3 Newswire.Net <http://www.mp3newswire.net>, January, 10, 2002.
- [6] MITRE, *Common Vulnerabilities and Exposures Database*, CAN-2001-1004, <http://cve.mitre.org>, August, 2001.
- [7] Singh, M., *Peering at Peer-to-Peer Computing*. *IEEE Internet Computing*, 5(1): 4-5, 2001.
- [8] Vamosi, R., *The Rise of P2P Worms*, ZDNet, <http://www.zdnet.com>, September, 18, 2002.

Usability and privacy: a study of Kazaa P2P file-sharing

Nathaniel S. Good
Information Dynamics Lab
HP Laboratories
1501 Page Mill Road
Palo Alto, CA 94304 USA
ngood@hpl.hp.com

Aaron Krekelberg
Office of Information Technology
University of Minnesota
kreke002@tc.umn.edu

ABSTRACT

P2P file sharing systems are rapidly becoming one of the most popular applications on the internet, with millions of users online exchanging files daily. While primarily intended for sharing multimedia files, programs such as Gnutella, Freenet, and Kazaa frequently allow other types of files to be shared. Although this has no doubt contributed to P2P filesharing's growing popularity, it raises serious security concerns about the types of files that users are aware of sharing with others. Users who accidentally or unknowingly allow their private or personal files to be shared risk disclosing their private information to other users on the network.

In this paper, we use a cognitive walkthrough as well as a laboratory user study to analyze the usability of the Kazaa file sharing user interface. We discover that the majority of the users in our study were unable to tell what files they were sharing, and sometimes incorrectly assumed they were not sharing any files when in fact they were sharing *all* files on their hard drive. We also looked at the current Kazaa network, and determined that a large number of users are currently sharing personal and private files without their knowledge, and from our dummy server we were able to see that other users are indeed taking advantage of this and downloading files such as "Credit Cards.xls" and email files.

Keywords

Privacy, peer-to-peer networks, security, usability, user studies

1. INTRODUCTION

The excitement around P2P systems has been encouraged by recent innovations that foster easier sharing of files, such as downloading simultaneously from multiple sources, and the sharing of many different file types as well as improvements to the usability of these clients. Of the current P2P systems, Kazaa is by far the most popular and widely used, with over 85 million downloads worldwide and an average of 2 million users online at any given time. The user interface (UI) for finding files is straightforward: you type a file into a textbox and from the results select a file to download. If sharing is enabled, the

files that you download are available to be downloaded by other users.

While facilitating file sharing and searching, the systems do a poor job of preventing users from sharing potentially personal files. Users attracted to the simplicity of downloading files provided by the P2P network can inadvertently allow access to their private data files, such as email, tax reports, work related spreadsheets and private documents. This is especially problematic in a single machine, multiple user environment, a setup that is typical of families sharing a single computer. In such a setting, a parent could have a secure VPN connection to a corporation for downloading and working on important confidential files, only to have them inadvertently shared by a teenage son or daughter, without either party's knowledge. This is not simply a theoretical problem but describes a scenario that is possible in the current reality. Our research shows that people are currently sharing and downloading personal files from Kazaa, and are capable of doing so with users oblivious to any private data being shared. Queries for personal files such as Inbox, data for financial applications, and .pst files (Outlook mail folders) returned numerous results.

In order to understand how this can take place, we researched the interactions between the users and the software to determine if usability issues could account for such fatal errors.

Recent literature examined usability guidelines for user interfaces for security applications. Whitten et al[9] looked into usability problems that affected users sending secure messages via PGP¹, and how inadequate design caused users to make fatal mistakes such as sending unencrypted mail that they felt were encrypted or sending people their private keys. Yee[10] has expanded on this work, and provides a list of guidelines and case studies for usability of security applications. His work is based on work done by Saltzer[7] which focused on understanding the design requirements for developing secure systems.

¹ PGP – pretty good privacy <http://www.pgp.com/>

Title	Artist	Progress	Status	Uploaded/Requested	Time Remaining	Speed	Filename
Inbox			Completed	2172Kb/2172Kb			Inbox.dbx
Inbox			Completed	1480Kb/1480Kb			Inbox.dbx
Inbox (1)			Completed	22764Kb/22764Kb			Inbox (1).dbx

Figure 1 Inbox.dbx files being downloaded from our dummy client by other Kazaa users

While Kazaa is not a security application, like PGP or personal firewall software, it nonetheless shares similar responsibilities and obligations to its users. It must help users ensure that private and personal data is not shared with others. We use an approach inspired by the success of Whitten et al [9] in identifying the flaws within PGP 5.0. We perform a cognitive walkthrough and a user study to analyze the interface of Kazaa and determine usability issues that could cause users to share files unintentionally with the Kazaa network. The results detailed below show that usability issues alone could account for unintentional file sharing. Indeed, we were able to determine from our user studies that it was possible for users to share all files on their hard drive and not even know it.

Credit Cards	Credit Cards.xls	Completed
Credit Cards	Credit Cards.xls	Completed
Credit Cards	Credit Cards.xls	Completed

Figure 2 “Credit Card.xls” files Kazaa users downloaded from our dummy client.

2. ABUSES ON KAZAA TODAY

We were curious to see how wide of a problem this was on the current Kazaa network, and whether users were currently taking advantage of these features to download private files from others. Kazaa operates on a closed protocol, so we were unable to determine the full extent of people sharing personal files, as we were unable to tell exactly how much of the network was being searched with every query.

Unintended Filesharing Among Kazaa users

In order to gather data on the prevalence of unintended file shares on Kazaa, we scripted searches to run every 1.5 minutes for a 12 hour period. We purposely limited ourselves to queries only, and did not download any user files to verify their contents. The targets of the searches were files that end in .dbx with particular emphasis on inbox.dbx. DBX files are Microsoft Outlook Express email files. This is a good indicator that users are unintentionally sharing files for several reasons. First, it is commonly found on Windows machines because it is packaged with Internet Explorer and Windows. Second, it contains private email correspondence that most users would not likely intend to share. Finally, users who have their inbox shared typically have other files shared that contain potentially private information.

The results of 443 searches in 12 hours showed that unintentional file sharing is quite prevalent on the Kazaa network. 61% of all searches performed in this test returned one or more hits for inbox.dbx. By the end of the 12 hour period 156 distinct users with shared inboxes were found.

To further demonstrate that this indicates unintentional file sharing, we examined 20 distinct cases of shares on the inbox.dbx file by manually using the “find more from same user” feature. 19 of the 20 users shared the other email files found in the default Microsoft Outlook Express installation (Sent Items, Deleted Items, Outbox, etc.) In addition, 9 users had exposed their web browser’s cache and cookies, 5 had exposed word processing documents, 2 had what appeared to be data from financial software and 1 user had files that belong in the system folder for windows.

Users Downloading Others Private Files

After we determined that users were indeed sharing private files, we were interested in whether other users on the Kazaa network were taking advantage of this fact and downloading files from others. We ran a dummy client populated with dummy files (such as Credit Cards.xls, Inbox.dbx, Outlook.pst and other types of private files) over a 24 hour period.

From our dummy server, we received a total of four downloads from four unique users for an Excel spreadsheets named “Credit Cards.xls” and four downloads from two unique users of an Inbox.dbx file (Figure 2).

3. USABILITY GUIDELINES

By looking at the Kazaa network, we were able to determine that abuses were occurring, and their frequency demonstrates that they were not isolated events.

Based on a list of security guidelines provided by Whitten et al[9], we have created a modified list of usability guidelines for Peer-to-Peer File sharing applications below.

Definition: Peer-to-Peer file sharing software is safe and usable if users:

1. are clearly made aware of what files are being offered for others to download.
2. are able to determine how to successfully share and stop sharing files.

3. do not make dangerous errors that can lead to unintentionally sharing private files ; and
4. are sufficiently comfortable with what is being shared with others and confident that the system is handling this correctly.

During the cognitive walkthrough and the user study, we paid close attention to whether or not the interface was able to meet these guidelines, and if not why were they inefficient.

4. SUMMARY OF COGNITIVE WALKTHROUGH

Recent versions of the Kazaa application have made some progress in addressing these issues. A default installation of Kazaa for users using the latest version of Kazaa 1.7.1 is relatively safe, it creates a shared file folder, assigns this as the default download file and indexes these folders for the My Kazaa library. Previous versions of Kazaa offered to search for files to share with users during the initial setup. The program would then start and search for files such as audio, video and image files. All of this is done through a wizard interface that walks the user through the steps of setting up an account or using an existing one, software agreement and installing add software. Whereas the default configuration in the past enabled sharing, the latest configuration of Kazaa comes with sharing disabled.

While a default setup is relatively safe, user modification of various settings are not. By adding or changing directories to be shared, there were potential interface issues that could create misunderstandings about what files the system was sharing with other users, regardless of the version of Kazaa that the user is using. There are a number of reasons why a user would change default settings. Three common scenarios are driven by a user's desire to save the files being downloaded to a different location, share more files with other users or add files to the My Media. In the following sections, we will walk through each of these scenarios and the various ways that Kazaa allows these to be accomplished. We will look at the various safeguards that Kazaa employs to prevent users from sharing private files or files that they do not want others to see, and describe where they fail.

Changing the Download file directory

In Kazaa, as in most P2P applications, the share directory provides the dual purpose of specifying the files that the user decides to share with the network (if the user decides to share files), and the place where these files will be stored. The shared directory is referred to as the download directory in Kazaa, and is managed through the Options menu, in the tool tab (Figure 4). Additionally, the Options->Tools tab also contains a checkbox for users to determine whether they would or would not like to share files with the Kazaa community. Users may type in the directory they would like to download files to, or alternately browse their file system and select the folder they would like to use to store downloaded files (Figure 3).

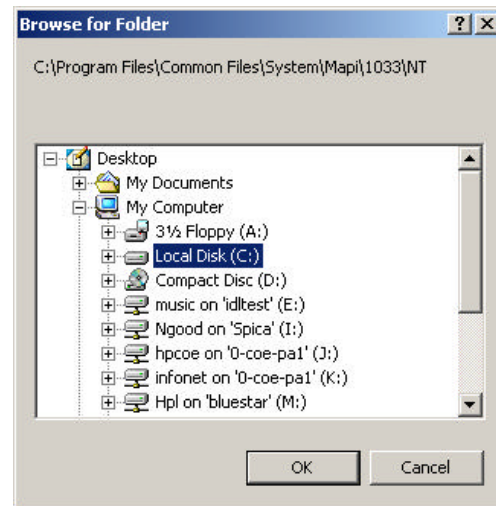


Figure 3 Browsing and selecting interface for the Shared/Download Folder. Note that the interface says browse for folder, and does not mention that the folders will be recursively searched for files.

If the user has decided to share files with others, then all files in this directory as well as the directories below it are recursively shared, and added to *My Media* files (Figure 11). The wording of the download folder (which doubles as the *My Shared Folder*) is confusing and misleading. The word “folder” is singular, implying one folder, and does not hint that all folders below it will be recursively selected to be shared with others. Also “download folder” implies that it will be used to store files that are downloaded and has nothing to do with sharing. It does not mention that this folder (and the folders and files underneath) will also be shared with others, if sharing is enabled.

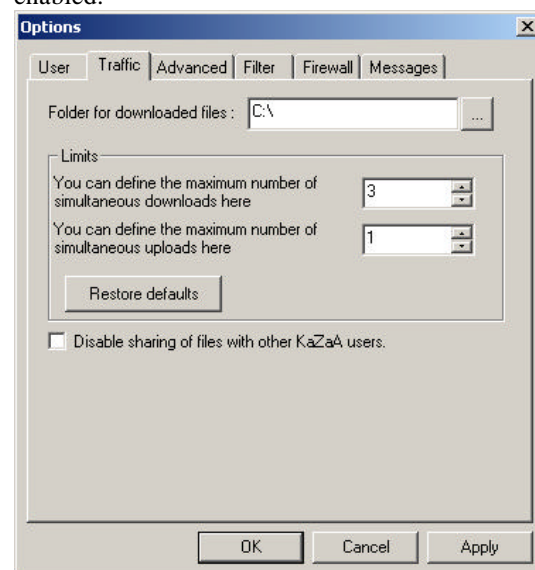


Figure 4 The traffic tab in the options folder. Here is where users specify the download and My Shared directory as well as toggle sharing of all files.

Another factor leading to user error is that hierarchical file systems can be very difficult for some users to navigate and conceptualize. Vicnete[8] demonstrated that users with low spatial ability have trouble navigating hierarchical file systems compared to those with high spatial ability. Conversations with computer trainers note that novice users are “notoriously bad” at navigating hierarchical file structures and prefer breadth as opposed to depth in browsing and searching for files or information. The trade offs between depth and breadth in hierarchical structures has been well studied by the psychological and human computer interaction communities [2,3,4,5]. Most reach the conclusion that breadth is better than depth. Systems such as that described in Placeless[6] recognize this problem, and attempt to alleviate it by allowing users to search intuitively based on file attributes rather than location. Anecdotally, Microsoft Windows and even Kazaa recognize this by placing shortcuts on the desktop to single file folders such as *My Shared Folder* and *My Documents*, allowing users one click access to file folders buried in hierarchies. By deciding to automatically recurse through directories for files, Kazaa assumes that all users have a detailed knowledge of their file system and its contents. We feel that this is an invalid assumption based on the variety of users using Kazaa. Having the default file sharing be recursive for all types of folders is confusing and misleading for users and should be avoided to alleviate misconceptions. At the very least, users should be given a choice to recursively add files or not when asked to share a folder.

Sharing files

Two interfaces that Kazaa provides for sharing folders are located in the Tools Menu, under “Find Shared Files” for version 1.7 and above. Selecting this menu item brings up a dialog box with two choices (Figure 5).



Figure 5 Selection interface to find or select shared folders.

One choice is to have Kazaa automatically discover files for the user, the other is for the user to browse her machine and determine what directories she would like to share. The find function uses a wizard interface to walk users through selecting drives to search, and selecting which folders to share after the process has been completed. In the latest version of Kazaa, it recommends folders containing documents (such as the My Documents folder), image files, and multi-media files, such as music and video, although it is not clear what criteria it uses in selecting files and folders. After searching the drives selected in the first step, it asks whether the user would like to share these directories or not using an array of checkboxes or a button to select/deselect all directories (Figure 6). A message above the list box tells users the steps that they will need to perform in order to stop sharing files that they decide to share in the folders that they select.

A weakness of this interface is that it does not list what criteria it uses in discovering folders to share. For example, it does not say what in My Documents it is going to share with the user on Kazaa, or why it found the My Documents folder interesting. The interface relies on the users knowledge of what is capable of being shared by a file sharing program and for what the program is looking. It presumes that users have perfect knowledge of what kinds of files that are contained in those folders and what will be shared. Also, as in all shared functions, these folders will be recursively searched for files and folders to share, and there is no indication that this will happen or way to toggle it on or off.

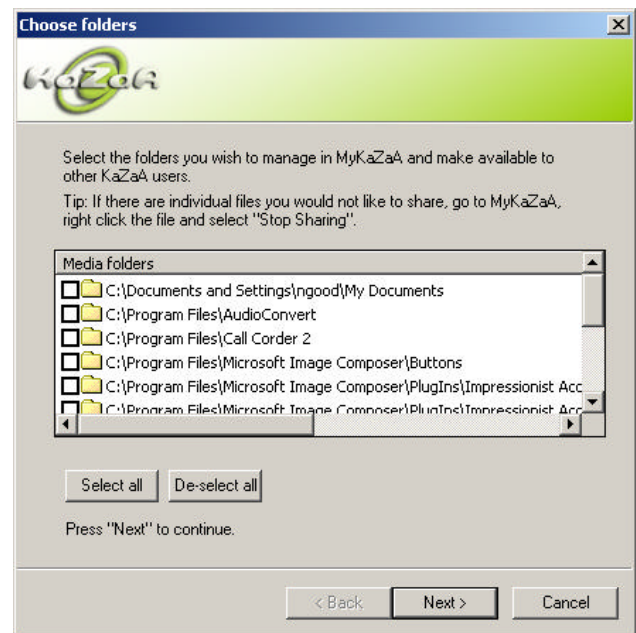


Figure 6 Search Interface

The “tip” portion is the only part of the interface that warns the user that they may share files that they would

rather not. It is unclear whether users would read this message, and if so, remember the instructions and places they need to go in order to stop sharing files that they would not like to have public. It also mentions that users must remove the files one-by one if they choose not to share them. Overall, while the search interface affords sharing more files, it makes browsing, searching and stopping sharing of files difficult and tedious.

The other function, which we will call the folder select function, allows the user to browse the current file system and select a folder or folders to share (Figure 9). Folders are shared by selecting a checkbox, and is turned off by deselecting the checkbox. The interface allows you to click and unclick directories, therefore sharing or not sharing them with others.

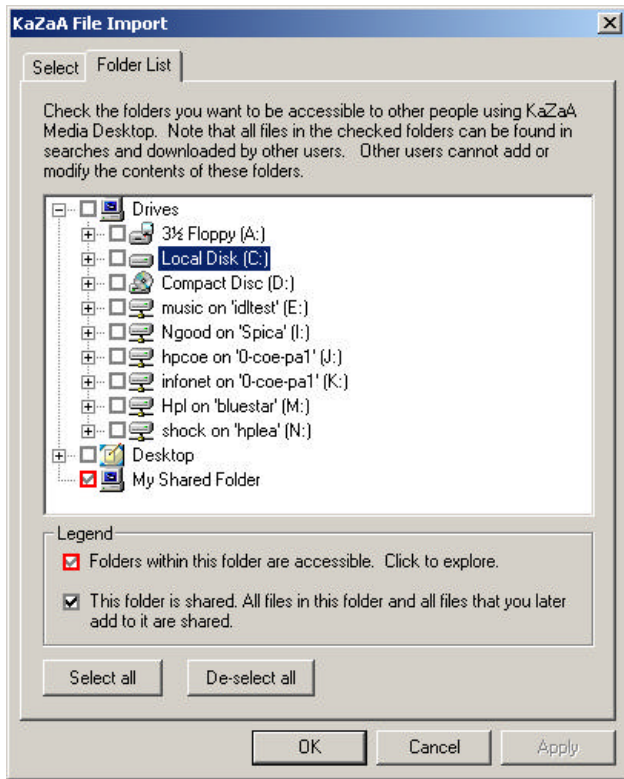


Figure 7 Folder Select Function to share or stop sharing folders

If a user selects a drive, (such as C, D drive) a message pops up (Figure 8) warning the user that this action will share all files with all Kazaa users for this drive. This warning will not appear again if any user on a given machine decides to check “Do not show this again”, and future users will not be able to see this warning.

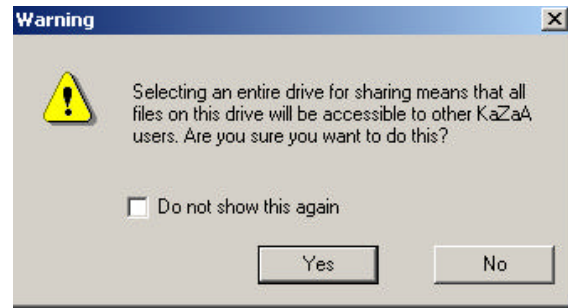


Figure 8 Warning to not share the entire folder from the Folder Select Function.

When a user selects a directory, then the directories below it are selected automatically for the user (Figure 9 and Figure 10).

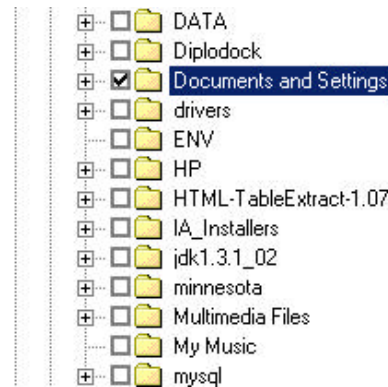


Figure 9 List of directories in the folder select function (figure 6). Documents and Settings is Selected.

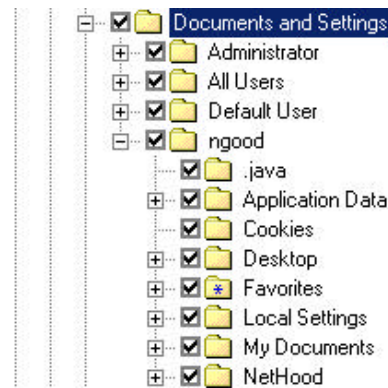


Figure 10 Expanded View of folders selected by selecting Documents and Settings.

We noticed that if file sharing was enabled through Figure 4 and the user had changed the download directory to something else, this change was not reflected in the folder select window, Figure 7. For example, if a user changed their download directory to C:\ and sharing is enabled, they are sharing their whole hard drive to others, and no warning like the one in Figure 8 is given. All of these files are

indexed by My Kazaa, but there is no indication in the folder select function (Figure 7) that the entire hard drive has been shared, as there is nothing checked next to the C:\ icon. We found this to be a very critical flaw that was definitely misleading. In effect, it allowed users to share anything through the download folder, and not be aware of it through the folder selection function. In the user studies conducted below, this error had serious repercussions on user expectations of shared folders and files.

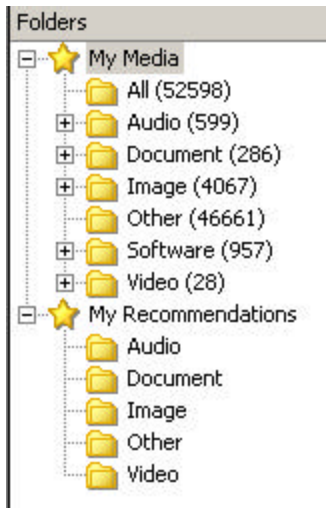


Figure 11 My Media Folder

Adding Files to the My Media Folder

Kazaa, like most file sharing programs, comes with a built in media player that allows playback of a variety of audio and video formats. Playback of these formats is done through the My Kazaa tab, which organizes files based on their content into file folders, similar to the interface provided by Microsoft Internet Explorer (Figure 11). To add files to My Media, they must be shared or included in the download directory as described above or through another button that “imports” files into My Media, using similar techniques as described above. Folders in My Media may be either shared or not, depending on whether the user has decided to share folders by selecting the checkbox in the Options->tool menu described above.

Files imported into the *My Media* folders can be individually turned on and off via a context menu or an icon above the file folders. The context menu is only activated for individual files, and does not work at the top folders or root folders of the directory structure. For example, if a user wanted to disable sharing of applications in the software folder, the only choice she would have would be to disable sharing entirely, or stop sharing each individual file. Also, there was no indication of exactly what folders were being shared on the users hard drive, which could potential confuse users as to the meaning of the contents contained in the My Media folders. In the

user studies we conducted below, the My Media folder was a source of general confusion. User opinions about its purpose and contents varied greatly and are described in detail below.

Uploading Files

During the walkthrough we examined the *Transfer File* interface that is used for users to determine what is currently being uploaded and downloaded from the Kazaa network. It consisted of two adjustable scrollable lists. Files being transferred to others are appended to the bottom of file transfer list, and the file transfer list is cleared every time Kazaa is restarted, erasing any past transactions. Users would therefore have to be very attentive to what is being transferred in Kazaa, in order to be aware of any unwanted file shares.

Overview of Results from the Cognitive Walkthrough

We summarize the results of the cognitive walkthrough below in relation to how well they satisfied each of the earlier proposed guidelines.

1. *Users should be made clearly aware of what files are being offered for others to download.*

We found downloading files to be straight forward, as was playing files from the media desktop. However, when selecting files to be shared from the file search interface (Figure 6), we noticed that the interface did not provide a means to view the files that were in the directories that it had discovered, nor did it reveal what kinds of files it was intending to share. Also, selecting a directory through any means (Figure 3, Figure 5, Figure 7) recursively shared all directories and files below it. It did not provide the user with a means to indicate whether they wanted to select all files and folders beneath the selected folder, or provide any indication to the user that the application would do this.

Additionally, the Kazaa client treats all files equally, whether they are Inbox.pst (the user’s mailbox) files, systems files, files in hidden directories, music files or navigation icons cached by a browser. All files are candidates for sharing, and it makes the default assumption that users would like to share all types of files. Not having built in distinctions and safeguards pushes the burden of safeguarding information onto the user.

2. *Users should be able to determine how to successfully share and stop sharing files.*

The brief “tips” message displayed in the file search interface (Figure 6) indicated how to deselect individual files that the user would not want to share in the *My Media* folder. Users are expected to have read this information, and remember it if they would like to stop sharing files later. Also, they will have to individually deselect files one at a time. The positioning of this text is meant to be helpful, but would be more so if the user was

allowed to select and deselect files to share at this point, rather than later.

The only place to stop sharing was located under two menus, and hidden in one tab labeled “Traffic.” It seems strange to have over three separate interfaces and multiple ways to share folders, but only one hard to find way to stop sharing. We feel that this function should be brought to the front of the interface, to allow users to easily identify whether they have sharing enabled or not, and toggle this as they see fit.

3. Users should not be able to make dangerous errors that can lead to unintentionally sharing private files

A particularly disturbing find was that files and folders shared through the download folder (Figure 3), were not indicated as shared in the Share Folders box (Figure 7). For example, if a user selected C:\ as their download folder and enabled sharing, then the folder selection function did not show that these files were being shared (Figure 7). By not coupling these views, the interface does not clearly establish a link between shared folders and download folders. Also, it could potentially mislead users into thinking that no items were being shared, when in fact they were.

4. Users should be sufficiently comfortable with what is being shared with others and confident that the system is handling this correctly

Whether files are shared or not, if they are imported they are included in the added to the *My Media* folder. The *My Media* folder serves two roles; it categorizes user media and multi-media for easy access and playability, but is also used to display what could be shared with others on Kazaa. In order for files to be part of the *My Media* library, all files in the media library have to be potentially shareable. Despite this fact, the only feedback available to the user on the current shared status is a cryptic icon next to the file in the folder list. From a global view, there was no way to tell if a folder was shared. To determine what is shared, users must use the detail view and tediously scroll through the list of files and observe the individual icons next to each file. This was problematic because users could assume that their media file contained a library of their personal items, which would only be true if the file sharing was turned off.

By not providing a way for users to manage and view the types of files and extensions being shared during the selection phase, the interface is very vulnerable to misunderstandings by relying too much on users understanding the assumptions the program has made in searching for files to share.

5. USER STUDY

Our user study was intended to determine whether the lack of coupling between shared items in the download folder and shared folder interfaces that we discovered in

the walkthrough would confuse users, and whether they would be able to tell what was being shared. The study was further designed to show whether users could determine which, if any, folders were being shared by the Kazaa application with other users.

Our users study consisted of 12 users. Ten of these users had used file-sharing applications before (such as Morpheus, Gnutella, Kazaa and Napster) and 2 had not. All the users spent over 10 hours a week on their computers.

User Task

For the user test, we were also interested in the users conceptions on the types of files that peer-to-peer filesharing applications could share, as well as whether they were able to perform the specified task. We asked the users to indicate what types of files that they knew could be shared over peer-to-peer networks, in addition to performing a specific task using Kazaa.

Users were asked to discover what files were being shared, if any, on a Kazaa media desktop running Kazaa version 1.7.1. Kazaa was preinstalled, and the download files option (Figure 4) was set to C:\. File Sharing was enabled, so all files on C:\ were shared. In order to prevent others from downloading our files, we set up Kazaa behind a firewall and blocked incoming requests to download files. This prevented others from actually accessing our files, but still allowed Kazaa to index all the files and provide them for sharing.

All users were given the same starting position, the Kazaa home page, and told to take as much time as they needed to determine if, and which, files or folders were allocated for sharing with other Kazaa users. They were given a short tutorial on file sharing, and the concept of a shared folder. They were allowed to only use the Kazaa interface, and at the end of the searching were asked to provide a clear answer of whether they thought files were being shared and if so, which folders they were. If they determined that files were being shared, we asked them to stop sharing them, and share only the My Shared Folder.

6. RESULTS

Survey

Only 2 users indicated correctly that all files could be shared. Most users agreed that music, software and movies could be shared (9 of remaining 10), where as only 1 of the remaining 10 users indicated correctly that it was possible to share office documents, source code files and email folders. After completing the task, some users were very surprised to learn that all files could be shared with others and some couldn't understand why. One user exclaimed, “You mean it shares *all* files?” and expressed concern about why it would be able to share anything other than multi-media files. The results from our survey demonstrate unequal expectations between Kazaa and the

users, and demonstrated a violation of the first guideline proposed earlier.

Task

Only 2 of the 12 users were able to determine correctly the files and folders that were being shared. Of those 2, both were able to turn off sharing completely using the “stop sharing feature” (Figure 4), but were not able to determine how to stop sharing a single given folder. Of the remaining users,

- 5 of 12 determined incorrectly that only the “My Shared Folder” was the only folder being shared, based on the information they saw from the folder select feature (Figure 7).
- 2 of 12 used the find files interface to search for folders they were sharing. When everything showed up unchecked (Figure 6), the users concluded incorrectly that nothing was being shared.
- 2 of 12 browsed help and used it to determine incorrectly that the only folder they could share was the “My Shared Folder”
- 1 of 12 was unable determine what folder was being shared after going through every menu item in the application and the help in the web interface. The user said that the files in My Media were probably being shared, but admitted that he couldn’t determine which folders.

During the study, many users found the initial interface difficult to navigate. Many users traversed the web interface to look for answers. In the help section, several users tried to use the “search” function, assuming incorrectly that it searched help and not the Kazaa network. Of the users who were able to make it to the menus above, only one was able to make a connection between the “download folder” (Figure 4) and the “My Shared Folder” described in the help and shown on the folder selection feature (Figure 7). Users had difficulty finding the menus above, and determining which items to select. One user later described the experience as a “buckshot approach” to find out what was where. The user mentioned that “he had no clue” where to look for shared folders, and resorted to looking through every menu item for something that made sense.

There was considerable confusion about the My Media directory. Less than half of the users thought that items in My Media were being shared with others, the rest either thought it held an archive of all media on the machine for personal use, or assumed it contained some shared and some unshared items. Only 3 users could determine which items were shared and which weren’t by looking at the file icons, but all were unsure of which folders in My Media

contained shared items and which contained items not being shared without browsing each individual folder.

7. SUGGESTIONS

Based on what we found in the surveys, user studies and cognitive walkthrough, we have several suggestions that may help improve the current interface. One suggestion would be to prohibit sharing of files that are not multimedia files. As most users in our study were unaware of the fact that they could share files other than multimedia, this would realign users expectations with the current reality. Another possibility is to make the default sharing limited to an explicit set of file types in line with users expectations, but allow advanced users to permit additional file sharing on a per file basis as long as these changes are explicit enough for all users to understand. We feel that current interface is weighted too heavily in favor of sharing files, and our users studies suggest that improvements can be made to create a balance between sharing files and protecting and preserving users privacy.

8. CONCLUSION

While the interface provided by Kazaa affords simple sharing and file download features we find that it’s sharing interface is problematic. The design makes too many assumptions about the users knowledge of file sharing, and fails all four of the proposed usability guidelines.

By providing several different locations and interfaces to manage file sharing and not connecting their information, users are not made aware of what files are being offered for others to download and are not able to determine how to successfully share and stop sharing files. Ambiguity and assumptions about recursion and types of files being shared allow users to make dangerous errors, such as sharing an entire hard drive. Finally, the confusing multiple purposes of the My Media interface cause users some confusion about what is actually being shared. Given the potential violation of user privacy and the current abuses that we noted above, it should be a top priority for file sharing applications to look into usability for security applications, and design their applications accordingly.

9. ACKNOWLEDGMENTS

We would like to thank the subjects as well as Eytan Adar, Rajan Lukose, Caesar Sengupta, Lada Adamic, Josh Tyler, Leslie Fine and Bernardo Huberman for their comments and support. We would also like to thank Marti Hearst, Paul Dourish and Victoria Bellotti for their help with related work. We would like to thank the Office of Information Technology at the University of Minnesota for allowing us to use their computers.

10. REFERENCES

1. Jacko, J. A. B Salvendy, G. (1996). Hierarchical menu design: Breadth, depth, and task complexity- Perceptual and Motor Skills, 82, 1187-120 1,
2. Kiger, J. I. (1984). The depth/breadth tradeoff in the design of menu-driven interfaces International Journal of Man-Machine Studies, 20,201-2 13.
3. Larson, K. and Czerwinski, M., Web page design: implications of memory, structure and scent for information retrieval, Conference proceedings on Human factors in computing systems, pp. 25-32, ACM
4. Milier, G. A. (1956). The magical number seven plus or minus two: Some limits on our capacity for processing information. Psychological Review, 63, 81-97.
5. Miller, D. P. (1981). The depth/breadth tradeoff in hierarchical computer menus. Proceedings of the Human Factors Society, 296-300.17.
6. Paul Dourish, Keith Edwards, Anthony LaMarca and Michael Salisbury. 1999. Presto: An Experimental Architecture for Fluid Interactive Document Spaces. ACM Transactions on Computer-Human Interaction, 6(2), 133-161.
7. Saltzer, J. H. and Schroeder, M. D.. The Protection of Information in Computer Systems. In Proceedings of the IEEE, vol. 63, no. 9, September 1975, pp. 1278-1308 (see <http://web.mit.edu/Saltzer/www/publications/protection/>).
8. Vincente, K.J. and R.C. Williges, Accommodating Individual Differences in Searching a Hierarchical File System. International Journal of man Machine Studies, 1988. 29
9. Whitten A. and Tygar, J. D.. Why Johnny can't encrypt. In Proceedings of the 8th USENIX Security Symposium, August 1999.
10. Yee, K.-P.. User Interaction Design for Secure Systems, University of California Berkeley Tech report, May 2002, Tech Report CSD-02-1184 Available at <http://www.sims.berkeley.edu/~ping/sid/>
11. Zaphiris, P. & Mtei, L. (1997). Depth vs Breadth in the Arrangement Web Links. Available at <http://otal.umd.edu/SHORE/bsO4/>