UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM – STAFF REPORT
PREPARED FOR REP. TOM DAVIS AND REP. HENRY A. WAXMAN
MAY 2003

FILE-SHARING PROGRAMS AND PEER-TO-PEER NETWORKS
PRIVACY AND SECURITY RISKS

WWW.REFORM.HOUSE.GOV | WWW.REFORM.HOUSE.GOV/MIN

TABLE OF CONTENTS

EXECUTIVE SUMMARY

At the request of Reps. Tom Davis and Henry A. Waxman, the chairman and ranking member of the Committee on Government Reform, the staff of the Government Reform Committee examined potential privacy and security risks associated with the use of popular peer-to-peer (P2P) file-sharing programs. This report summarizes the results of the congressional staff investigation.

File-sharing programs are popular Internet applications that allow users to download and share electronic files. Since the first such program, Napster, was shut down by court order, newer file-sharing programs have taken its place and become one of the fastest-growing uses of Internet technology. The most popular file-sharing program, Kazaa, typically has four million simultaneous users. Other popular file-sharing programs include Morpheus, iMesh, BearShare, LimeWire, and Grokster.

Unlike Napster, which was limited to trading of audio files, the new file-sharing programs allow users to download any type of file from other computers connected to the network. This powerful feature creates unique privacy and security risks. In fact, file-sharing programs can potentially make every file on a computer available to millions of other users on the network.

The report finds:

- **Many users of file-sharing programs have inadvertently made highly personal information available to other users.** Committee investigators found that file-sharing programs could be used to obtain tax returns, medical records, attorney-client communications, and personal correspondence from P2P users. A search of one P2P network found at least 2,500 Microsoft Money backup files, which store the user's personal financial records, available for download.

- **P2P file-sharing software tested by Committee investigators introduce "spyware" or "adware" onto users' computers.** In Committee testing, spyware and adware programs, which collect personal information for marketers, were bundled with file-sharing programs. These spyware and adware programs caused computer difficulties, including increased "pop-up" advertisements, increased targeted spam e-mail, unusual browser activity, new and unwanted desktop software installations, and, in some instances, software conflicts and system crashes.

- **P2P file-sharing software can spread viruses, worms, and other malicious computer files.** Computer security experts consulted by the Committee reported that file-sharing programs can place users' computers at additional

risk for viruses and other malicious files due to increased connectivity, flaws in software design, and potential for quick distribution of malicious programs.

BACKGROUND

The Rise of File-Sharing Programs

File-sharing, the trading of electronic files between two or more users, was first popularized in the 1990s by the software company Napster. Napster provided free and easy-to-use software through which users could connect their computers to one another — known as a peer-to-peer (P2P) networking — to trade music files. At its peak in February 2001, Napster had as many as 1.6 million simultaneous users trading music through its centralized servers.[1] In 2000, the recording industry initiated litigation against Napster to protect its copyrights. This litigation resulted in a federal court injunction against Napster, which forced the company to shut down its centralized servers in July 2001.

Popularity of P2P File-Sharing Software Programs

According to a company representative, the Kazaa P2P file-sharing program is on track to become the most popular software download ever by June 2003.

Source: Philip Corwin, Kazaa representative (May 13, 2003).

Following the demise of Napster, a multitude of new file-sharing software programs have arisen. These new programs differ from Napster in two important ways. Whereas Napster limited users to trading electronic music files, these new programs allow users to share any kind of file, including videos and images, as well as text files. And whereas the Napster network was centralized around one computer server which tracked the trading of files, these new programs allow direct user-to-user file trading.

The new file-sharing programs include programs such as Kazaa, Morpheus, and iMesh. They first became available in 2001. Since then, their popularity has surged. In total, six of the most popular file-sharing programs have been downloaded more than 400 million times. Kazaa, the most popular file-sharing program, has been downloaded more than 220 million times, 22 million times in the last two months alone. It is currently the most popular software download on Download.com, a software clearinghouse.[2] *See* Table 1.

[1] Neo-Napsters Proliferate in the Wake of Napster's Demise, *Broadband Week* (Aug. 2001).

[2] Download.com (May 13, 2003) (online at http://download.com.com/3101-2001-0-1.html?tag=dir).

At any given time, these file-sharing programs are being used by millions of people. On a recent day, for example, Kazaa had more than four and a half million users connected to the network simultaneously — more than two and a half times the number of users Napster had at its peak.[3]

Many of the users of these new file-sharing programs are under the age of 18. Research done by Peter D. Hart Research Associates has found that of those who download files through file-sharing programs, 41% are between the ages of 12 and 18.[4] Other data shows that nearly 44% of Americans between the ages of 12 and 17 have downloaded music files from the Internet, including through file-sharing programs.[5]

Table 1
Downloads of Popular File-Sharing Program

File-Sharing Program	*Total Downloads*
Kazaa	222,591,000
Morpheus	111,012,000
iMesh	48,807,000
BearShare	18,269,000
LimeWire	15,336,000
Grokster	7,829,000

Source: Download.com (May 8, 2003) (online at http://download.com.com/3101-2001-0-1.html?tag=dir).

The Purpose of This Report

Almost all news coverage of file-sharing focuses on just one issue: the ability of users to trade copyrighted music, movies, and videos. Reps. Tom Davis and Henry A. Waxman, the chairman and ranking member of the Committee on Government Reform, requested this report to examine another aspect of file-sharing: the potential privacy and security risks posed by the use of today's popular P2P file-sharing programs. An earlier report for Reps. Davis and Waxman examined the exposure of children who use P2P file-sharing programs

[3] On May 7, 2003, at 4:10 p.m., Kazaa had 4,614,035 concurrent users.

[4] Peter D. Hart Research Associates, in-house research conducted for Recording Industry Association of America (undated).

[5] *Digital Music Behavior Continues to Evolve*, Ipsos-Reid (Feb. 1, 2002) (online at www.ipsos-reid.com/pdf/publicat/docs/TEMPO_DldingPrevalence.pdf).

to pornographic content, such as x-rated videos.[6]

File-sharing programs raise privacy and security issues because at the same time that they allow users to download files from other computers, they also allow others to download files from the user's computer. Within minutes of installing a P2P file-sharing program, new P2P users can find their electronic files being downloaded from their computers by other users on the network. The ease with which files can be shared on the P2P networks raises concerns about the potential sharing of personal information, especially by users unfamiliar with the potential risks. According to a June 2002 study by researchers working for HP Laboratories:

> 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.[7]

Privacy and security issues are also raised by the bundling of third-party software programs known as "spyware" and "adware" with file-sharing programs and by the potential for the spread of viruses, worms, and other malicious computer files on the peer-to-peer networks.

At the request of Reps. Davis and Waxman, this report seeks to address three issues:

1. Is there evidence that P2P users are sharing personal documents on the P2P networks? If so, what are possible reasons that may contribute to the sharing of personal information?
2. Are third-party software programs known as "spyware" and "adware" bundled with popular P2P file-sharing programs? If so, what are the privacy and security concerns associated with their installation?
3. Does the use of P2P file-sharing programs pose a significant risk of infecting a computer with viruses, worms, or other malicious computer programs beyond that posed by web use?

[6] Committee on Government Reform, *Children's Exposure to Pornography on Peer-to-Peer Networks* (Mar. 2003).

[7] Information Dynamics Laboratory, HP Laboratories Palo Alto, *Usability and Privacy: A Study of Kazaa P2P File-Sharing* (June 5, 2002).

This report focuses on the privacy and security issues raised by current versions of peer-to-peer file-sharing programs. It is not intended to reach conclusions about the underlying peer-to-peer file-sharing technology itself.

FINDINGS

P2P Users Are Inadvertently Sharing Highly Personal Information

The Committee staff found that users of file-sharing programs are making personal files and information – including tax returns, social security numbers, and other personal and financial information – available for sharing on P2P networks. The Committee testing was done using the Kazaa program. Consistently, personal information was easily found, often within the first set of results returned by simple keyword searches.

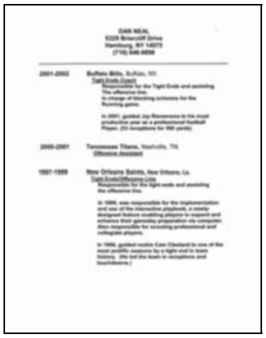
The kinds of specific files found included:

- Completed tax returns with social security numbers, names and social security numbers of spouses and dependents, income and investment information
- Medical files, including medical records of military personal and military medical supply records
- Confidential legal documents such as attorney-client communications regarding divorce proceedings and living wills
- Personal correspondence, including entire e-mail inboxes of individuals
- Business files, including contracts and personnel evaluations
- Political records, including campaign and political records and private correspondence with constituents
- Resumes with personal addresses, contact information, job histories, salary requirements, and references

Figure 1 displays some examples of the kinds of personal information about individuals that are available for sharing and downloading on the Kazaa network.

Figure 1

Examples of Personal Files Found on Peer-to-Peer Networks

Completed 1040 Tax Form Youngstown, OH	**Completed 1040 Tax Form Adamstown, MD**	**1040 Tax Form Cordova, TN**	**Completed 1040 Tax Form Walla Walla, WA**
Narcotics Inventory of Naval Ship	**Navy Medical Record of Service Member**	**Letter from Client to Attorney Regarding Divorce Proceedings**	**Living Will**
			
Resume of NFL Coach	**Business Correspondence Regarding Personnel Evaluation**	**Letter from State Senator to Constituent**	**Personal E-mail Inbox**

Source: Committee staff test using Kazaa file-sharing program (April—May 2003) (*images blurred to obscure personal details)*.

Once one personal file is discovered on a P2P user's computer, a feature on Kazaa called "Find More from Same User" will reveal every file being shared on that user's computer. Use of this feature can result in the disclosure of a wide range of highly personal information about the user. Table 2 displays examples of the kinds of personal files found by Committee staff using this feature.

Table 2

Examples of Personal Files Being Shared by Selected P2P Users Found Using Kazaa's 'Find More from Same User' Feature

Kazaa User	***Personal Files Shared by User***
User 1	• Completed 1040 tax return • Correspondence from the office of a state senator to constituents • Internal correspondence on state political organization
User 2	• Internal business records • Sensitive business correspondence, including memos on board of directors decision making
User 3	• Navy medical records • Military medical manuals • Shipboard medical supply inventories • Military information on chemical warfare • Mass casualty drill guidelines
User 4	• Correspondence with realtor on home buying • Correspondence with attorney on child's legal situation, divorce proceedings
User 5	• Personal correspondence including job experience at U.S. embassy in South America • Resume and cover letter • Personal statement • Recommendation letters
User 6	• Completed 1040 tax return • Job resignation letter including details of nursing home employment
User 7	• Two resumes of family members • My Money backup file
User 8	• Resume • Outlook Inbox file

Source: Committee staff test using Kazaa file-sharing program (April—May 2003).

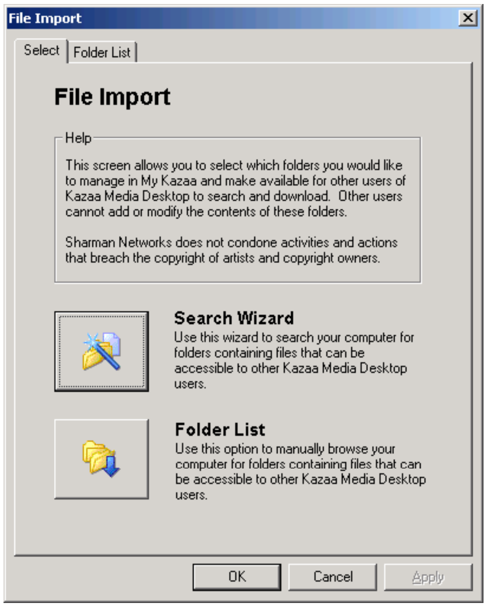
To estimate the scope of sharing of private financial records, the Committee asked MediaDefender, a company with expertise in peer-to-peer networks, to count the number of Microsoft Money backup files available for download. Microsoft Money is a popular financial software program. Its backup file contains the personal financial data entered by the user and can include online banking account numbers and credit card account numbers. In the program's default configuration, the backup file is saved to the "My Documents" folder on a user's computer.

MediaDefender monitored the FastTrack network for one five-day period. This is the network which is used by Kazaa, iMesh, and Grokster. MediaDefender found 2,504 unique Microsoft Money backup files available for sharing and download over this period.[8]

There are several possible causes of the unintentional sharing of personal information over P2P networks. Many users may inadvertently share personal files on the P2P network as a result of how the program is configured on their computers during the installation process. The installation process for Kazaa, the most popular file-sharing program, creates a shared folder on the user's computer in which the uploaded and downloaded files are placed by default. The creation of this shared folder would not expose personal information on the user's computer to other network users unless the user moved the information to the shared folder.

The next step of the Kazaa installation process, however, gives the user two options by which they can select which files to share on the network: a Search Wizard or a Folder List. *See* Figure 2.

Figure 2
Kazaa Installation File Import Process



File Import

Help

This screen allows you to select which folders you would like to manage in My Kazaa and make available for other users of Kazaa Media Desktop to search and download. Other users cannot add or modify the contents of these folders.

Sharman Networks does not condone activities and actions that breach the copyright of artists and copyright owners.

Search Wizard
Use this wizard to search your computer for folders containing files that can be accessible to other Kazaa Media Desktop users.

Folder List
Use this option to manually browse your computer for folders containing files that can be accessible to other Kazaa Media Desktop users.

Source: Committee staff test (May 13, 2003).

If the user elects the Search Wizard option, as many users will, the installation program will search the user's computer and select for sharing any folders containing image, music, or video

[8] MediaDefender, original research conducted for the Committee on Government Reform (May 14, 2003).

files. This creates a significant risk of inadvertent sharing of information. For example, a user who uses the Search Wizard option would expose the entire contents of his or her “My Documents” folder to file-sharing if the user had stored any music or image files in that folder.

Unintentional sharing of personal information can also result from the sharing of one computer among several users. For example, a teenager sharing a computer with his or her parents may elect to make the entire computer available for file sharing without thinking about the types of files stored on the computer by his or her parents.

To some extent, “frequent user” preferences associated with file-sharing programs may also encourage sharing of personal information. Kazaa users receive a “Participation Level” based on the numbers of files they share that other users download, and users with higher participation levels enjoy higher priority on popular downloads. LimeWire users who choose to not share files on the network are labeled as “freeloaders” and can be prevented by other users from downloading files. These features may induce users to configure their file-sharing programs to maximize the number of files available for sharing.

P2P File-Sharing Programs Introduce Spyware and Adware to User Computers

Adware “installs itself after you click ‘I agree’ or legally consent to having the program on your computer. The software might monitor your Web browsing habits or ask for your demographic data to generate ‘targeted ads’ based on your interests.”

Spyware “often installs itself without your consent. The software might monitor your Web browsing habits or record your passwords, credit card information or other e-commerce data.”

Source: CNET News.com (online at http://news.com.com/2009-1023-885144.html).

In the course of program testing, Committee staff installed six popular P2P file-sharing programs: Kazaa, Morpheus, iMesh, BearShare, LimeWire, and Grokster. In each case, the default installation of these popular programs installed third-party programs commonly referred to as “spyware” or “adware” on the Committee computer. Both spyware and adware programs monitor the user’s web browsing habits and collect other personal data.

The specific spyware and adware programs installed on the Committee computer included Cydoor, eZula, Gator, Hotbar, SaveNow, and Xupiter. Installation of Kazaa on the Committee computer, for example, resulted in the installation of Cydoor and SaveNow, software programs which track a user’s e-mail address and data on his or her Internet browsing activity. [9]

Installation of LimeWire resulted in the installation of Xupiter, a particularly virulent spyware program. This program, which was also for a time bundled with Grokster, has been called "the most evil thing on the Internet" by Wired Magazine.[10] Like other spyware and adware programs, it can redirect a user's homepage to a different website, install a new browser toolbar, insert entries into the user's browser bookmark list, reinstall itself after uninstallation, and ultimately crash a user's system.[11]

The spyware and adware programs bundled with file-sharing programs caused numerous problems on the Committee computer systems, including browser redirection and networking difficulties. In fact, one Committee computer was rendered inoperable by software conflicts caused by the programs bundled with the P2P file-sharing programs. On this computer, even the computer technicians employed by the House of Representatives were unable to remove the offending programs completely. These experts suggested hard drive reformatting as the only way to resolve the resulting computer difficulties.[12]

Spyware and adware programs are bundled with file-sharing programs in order to generate revenue for the programs. PC Magazine reported that it is through spyware and adware that "file-sharing vendors make money while not charging for their products. In a sense, you are paying, but the coin is privacy, not money."[13]

Kazaa's policy on spyware, available on the Kazaa.com website, states: "Kazaa Media Desktop contains banner advertising and the option to install other third party applications in order to remain free to the user. Sharman Networks [parent company of Kazaa] does not condone the use of 'spyware' and does not use 'spyware' in Kazaa Media Desktop." Kazaa then defines spyware as software which operates on a user's computer "without their knowledge or explicit

[9] Safersite.com (online at www.safersite.com/PestInfo/C/Cydoor.asp) (assessed May 14, 2003); Computer Incident Advisory Capability, United States Department of Energy (online at www.ciac.org/ciac/techbull/CIACTech02-004.shtml) (accessed May 14, 2003).

[10] *Xupiter Mongers Deal Spam, Scams*, Wired.com (Feb. 5, 2003) (online at www.wired.com/news/infostructure/0,1377,57553,00.html).

[11] *Users Fume at Grokster 'Drive-by Download'*, Vnunet.com (March 3, 2003) (online at www.vnunet.com/News/1138433).

[12] Testing was done while computers were not connected to the House network in order to protect the privacy and security of Committee files.

[13] *Spyware—It's Lurking on Your Machine*, PC Magazine (Apr. 22, 2003) (online at www.pcmag.com/article2/0,4149,977889,00.asp).

permission." However, Kazaa users agree to the monitoring software bundled with Kazaa when they agree to Kazaa's extensive end-user license agreement.[14]

P2P File-Sharing Programs Can Spread Viruses, Worms, and Other Malicious Computer Files

Another privacy and security issue that has been associated with file-sharing programs is the risk of contracting a computer virus, worm, or other malicious computer file. According to news reports, eight worms infected P2P networks between May and September 2002 alone.[15] For example, the Benjamin worm, which created and shared new Kazaa folders, masked itself as popular music and other multimedia files, such as "Metallica – Until it Sleeps" and "Johann Sebastian Bach – Brandenburg Concerto No 4."[16]

To assess these security and privacy risks, the Committee staff contacted experts in computer security in academia and the private sector. These experts expressed significant concern about security vulnerabilities associated with file-sharing programs.

Kevin Rowney, Chief Technology Officer of Vontu Incorporated, an independent company with expertise in corporate network security, said that the presence of P2P programs on networked computers "poses a set of potentially serious threats to corporate networks" including viruses and worms. In Mr. Rowney's opinion, "banning P2P systems is definitely part of any reasonable best-practices approach to network security."[17]

Virus: "A virus is a manmade program or piece of code that causes an unexpected, usually negative, event. Viruses are often disguised as games or images with clever marketing titles."

Worm: "Computer worms are viruses that reside in the active memory of a computer and duplicate themselves. They may send copies of themselves to other computers."

Trojan Horse: "A Trojan horse program is a malicious program that pretends to be a benign application; a Trojan horse program purposefully does something the user does not expect."

Source: McAfee.com (online at www.mcafee.com/anti-virus/default.asp).

[14] Kazaa.com (accessed May 7, 2003) (online at www.kazaa.com/us/privacy/spyware.htm).

[15] *The Rise of P2P Worms--and How to Protect Yourself*, ZDNet.com (Sept. 8, 2002) (online at www.zdnet.com/anchordesk/stories/story/0,10738,2880466,00.html).

[16] *Benjamin a Ploy for Profit*, About.com (accessed May 7, 2003) (online at http://antivirus.about.com/library/weekly/aa052002a.htm).

[17] Communication with Committee staff (May 13, 2003).

Dr. John Hale, Director of the Center for Information Security at the University of Tulsa, told the Committee that "several factors conspire to make the risks induced by security vulnerabilities in P2P file-sharing clients much more serious" than the risks of surfing the web. Dr. Hale said that these factors included the increased connectivity of computer systems running P2P programs, the ability of widespread dissemination from computer to computer, and the fact that "P2P file-sharing networks expose systems to untrusted hosts and software, and offer little in the way of protection."[18]

Another feature that can induce security risks is the ability of these programs to circumvent firewalls. P2P file-sharing programs, like all Internet applications, connect a computer to an outside network through specific computer ports; network firewalls can block the use of certain Internet applications by blocking access to the specific port known to be used by that application. Popular file-sharing programs, Kazaa among them, have been reprogrammed to attempt accessing the Internet through a number of different ports as a way of maneuvering around network firewalls and the network security protections they provide. According to Jeff Schiller, Network Manager at Massachusetts Institute of Technology, the makers of these P2P programs "continue to modify and adapt their programs with the apparent goal, among others, of subverting attempts to control them."[19]

CONCLUSION

P2P file-sharing programs are popular Internet applications that allow users to download and share electronic files. There are potential privacy and security risks associated with the use of P2P file-sharing programs. Many users of P2P file-sharing programs have inadvertently made highly personal information available to other users. P2P file-sharing programs also introduce spyware and adware – programs which collect personal information for marketers – onto users' computers. And P2P file-sharing programs can place users' computers at additional risk for viruses and other malicious files due to increased connectivity, flaws in software design, and potential for quick distribution of malicious programs.

[18] Communication with Committee staff (May 14, 2003).

[19] Written testimony submitted to the Committee on Government Reform (May 13, 2003).