United States General Accounting Office

GAO

Testimony

Before the Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10 a.m. EST
on Thursday
March 13, 2003

FILE-SHARING PROGRAMS

Child Pornography Is Readily Accessible over Peer-to-Peer Networks

Statement of Linda D. Koontz
Director, Information Management Issues

G A O
Accountability * Integrity * Reliability

GAO-03-537T

March 13, 2003

FILE-SHARING PROGRAMS

Child Pornography Is Readily Accessible over Peer-to-Peer Networks

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-537T, a testimony before the 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. GAO's report on the results of this work (GAO-03-351) is being released today along with this testimony.

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.

http://www.gao.gov/cgi-bin/getrpt?GAO-03-537T

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

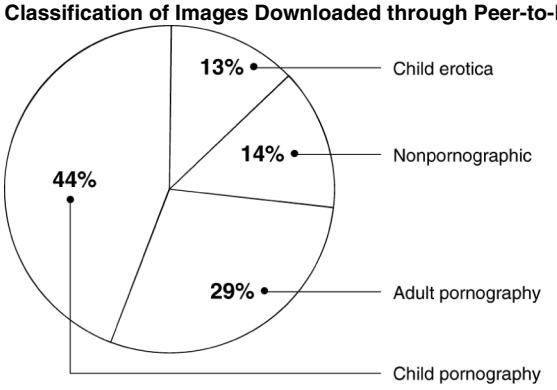
What GAO Found

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 consistent 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 reports 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.

Mr. Chairman and Members of the Committee:

Thank you for inviting us to discuss the results of our work on the availability of child pornography on peer-to-peer networks, which we provided to you in a report being released today.[1]

In recent years, child pornography has become increasingly available as it has migrated from magazines, photographs, and videos to the World Wide Web. As you know, a great strength of the Internet is that it includes a wide range of search and retrieval technologies that make finding information fast and easy. However, this capability also makes it easy to access, disseminate, and trade pornographic images and videos, including child pornography. As a result, child pornography has become accessible through Web sites, chat rooms, newsgroups, and the increasingly popular peer-to-peer technology, a form of networking that allows direct communication between computer users so that they can access and share each other's files (including images, video, and software).

As requested, in my remarks today, I summarize the results of our review, whose objectives were 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.

We also include an attachment that briefly discusses how peer-to-peer file sharing works.

Results in Brief

It is easy to access and download child pornography over peer-to-peer networks. We used KaZaA, a popular peer-to-peer file-sharing program,[2] to search for image files, using 12 keywords known to be associated with

[1] U.S. General Accounting Office, *File-Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography*, GAO-03-351 (Washington, D.C.: Feb. 20, 2003).

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

child pornography on the Internet.[3] Of 1,286 items identified in our search, about 42 percent were associated with child pornography images. The remaining items included 34 percent classified as adult pornography and 24 percent as nonpornographic. In another KaZaA search, the Customs CyberSmuggling Center used three keywords to search for and download child pornography image files. This search identified 341 image files, of which about 44 percent were classified as child pornography and 29 percent as adult pornography. The remaining images were classified as child erotica[4] (13 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 disseminating child pornography. Since 2001, when the center began to track reports of child pornography on peer-to-peer networks, such 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 can be inadvertently exposed to pornography, including child pornography. In searches on innocuous keywords likely to be used by juveniles, we obtained images that included a high proportion of pornography: in our searches, the retrieved images included adult pornography (34 percent), cartoon pornography[5] (14 percent), and child pornography (1 percent); another 7 percent of the images were classified as child erotica.

We could not quantify the extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks. Law enforcement agencies that work to combat child exploitation and child pornography do not track their resource use according to specific Internet technologies. However, law enforcement officials told us that as they receive more tips concerning child pornography on peer-to-peer networks, they are focusing more resources in this area.

[3] The U.S. Customs CyberSmuggling Center assisted us in this work. Because 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.

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

[5] Images of cartoon characters depicting sexually explicit conduct.

Background

Child pornography is prohibited by federal statutes, which provide for civil and criminal penalties for its production, advertising, possession, receipt, distribution, and sale.[6] Defined by statute as the visual depiction of a minor—a person under 18 years of age—engaged in sexually explicit conduct,[7] child pornography is unprotected by the First Amendment,[8] as it is intrinsically related to the sexual abuse of children.

In the Child Pornography Prevention Act of 1996,[9] Congress sought to prohibit images that are or appear to be "of a minor engaging in sexually explicit conduct" or are "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." In 2002, the Supreme Court struck down this legislative attempt to ban "virtual" child pornography[10] 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 of prosecuting those who produce and possess child pornography. Defendants may claim that pornographic images are of "virtual" children, thus requiring the government to establish that the children shown in these digital images are real.

[6] See chapter 110 of Title 18, United States Code.

[7] *See* 18 U.S.C. § 2256(8).

[8] See *New York v. Ferber*, 458 U.S. 747 (1982).

[9] Section 121, P.L. 104-208, 110 Stat. 3009-26.

[10] According 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 exists today to alter images to disguise the identity of the real child or make the image seem computer-generated, producers and distributors of child pornography may try to alter depictions of actual children in slight ways to make them appear to be "virtual" (as well as unidentifiable), thereby attempting to defeat prosecution. Making such alterations is much easier and cheaper than building an entirely computer-generated image.

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.[11] With the advent of the Internet, however, both the volume and the nature of available child pornography have changed significantly. 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 led to a proliferation of child pornography on the Internet.

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.[12] Today, child pornography is available through virtually every Internet technology (see table 1).

[11]John 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)

[12] Frederick 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.[13]

Web sites. According to recent estimates, there are about 400,000 commercial pornography Web sites worldwide,[14] with some of the sites selling pornographic images of children. The child pornography trade on the Internet is not only profitable, it has a worldwide reach: recently a child pornography ring was uncovered that included a Texas-based firm providing credit card billing and password access services for one Russian and two Indonesian child pornography Web sites. According to the U.S.

[13] According 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.

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

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 also provide 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.

Peer-to-peer networks. Although peer-to-peer file-sharing programs are largely known for the extensive sharing of copyrighted digital music,[15] they are emerging as a conduit for the sharing of pornographic images and videos, including child pornography. In a recent study by congressional staff,[16] a single search for the term "porn" using a file-sharing program yielded over 25,000 files. 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. [17]

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.

[15] According 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.

[16] Minority 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)

[17] Michael 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)

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 Homeland Security	U.S. Customs Service CyberSmuggling Center[a, b]	Conducts international child pornography investigations as part of its mission to investigate international criminal activity conducted on or facilitated by the Internet.
Department of the Treasury	U.S. Secret Service[a]	Provides forensic and technical assistance in matters involving missing and sexually exploited children.

Source: GAO.

[a]Agency has staff assigned to NCMEC.

[b]At the time of our review, the Customs Service was under the Department of the Treasury. Under the Homeland Security Act of 2002, it became part of the new Department of Homeland Security on March 1, 2003.

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 staff assigned directly to NCMEC as analysts.[18]

[18] According to the Secret Service, its staff assigned to NCMEC also includes an agent.

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).[19]

- 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 other organizations have responsibilities regarding child pornography: the Customs Service (now part of the Department of Homeland Security) and the Secret Service in the Department of the Treasury.

- 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 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.

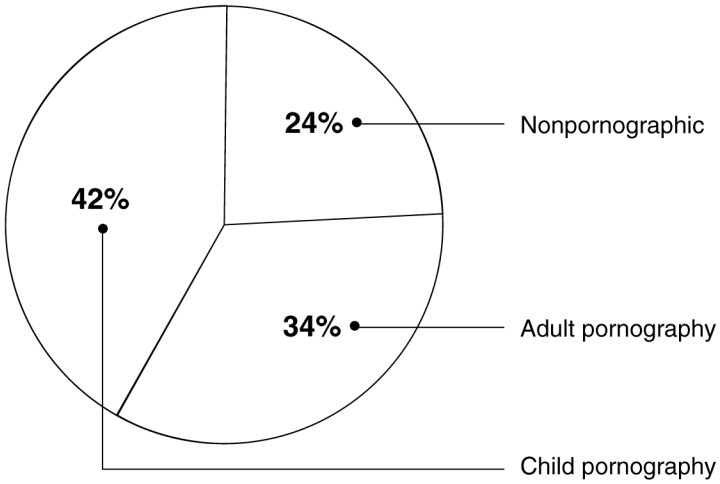
[19] Two additional Justice agencies are involved in combating child pornography: the U.S. Attorneys Offices and the Office of Juvenile Justice and Delinquency Prevention. The 94 U.S. Attorneys Offices can prosecute federal child exploitation-related cases; the Office of Juvenile Justice and Delinquency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

- 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.

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 keywords[20] showed that 543 (about 42 percent) of the images had titles and file names associated with child pornography images.[21] 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.

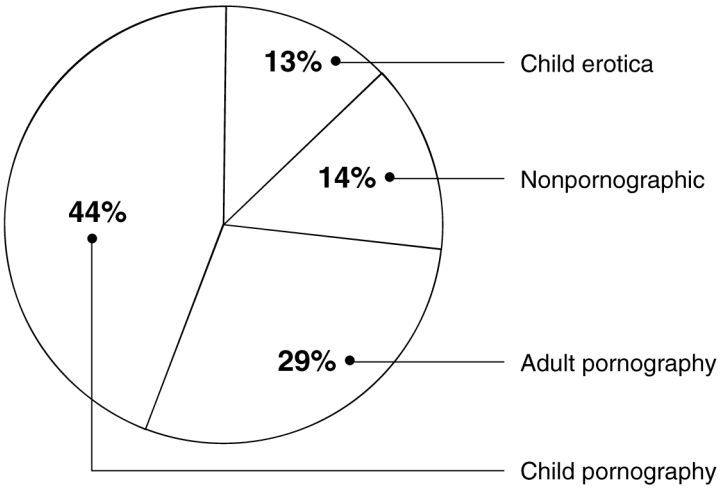
[20] The 12 keywords were provided by the Cybersmuggling Center as examples known to be associated with child pornography on the Internet.

[21] We 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.

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).

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

	Number of tips				
Technology	**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

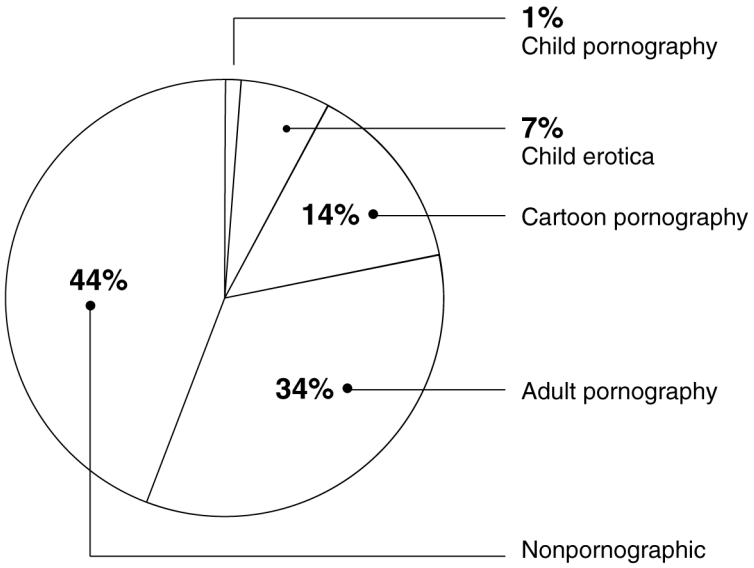
Juvenile users of peer-to-peer networks face a significant risk of inadvertent exposure to pornography when searching and downloading images. In a search using innocuous keywords likely to be used by juveniles searching peer-to-peer networks (such as names of popular singers, actors, and cartoon characters), almost half 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 likely to 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. These searches produced 157 files, some of which were duplicates. From these 157 files, the analyst was able to download 177 images.

Figure 3 shows our analysis of the CyberSmuggling Center's classification of the 177 downloaded images. We 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 (44 percent) 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.

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. Table 4 shows the levels of funding related to child pornography issues that the primary organizations reported for fiscal year 2002, as well as a description of their efforts regarding peer-to-peer networks in particular.

Table 4: Resources Related to Combating Child Pornography on Peer-to-Peer Networks in Fiscal Year 2002

Organization	Resources[a]	Efforts regarding peer-to-peer networks
National Center for Missing and Exploited Children	$12 million to act as national resource center and clearinghouse for missing and exploited children $10 million for law enforcement training $3.3 million for the Exploited Child Unit and the CyberTipline $916,000 allocated to combat child pornography	NCMEC referred 913 tips concerning peer-to-peer networks to law enforcement agencies.
Federal Bureau of Investigation	$38.2 million and 228 agents and support personnel for Innocent Images Unit	According to FBI officials, they have efforts under way to work with some of the peer-to-peer companies to solicit their cooperation in dealing with the issue of child pornography.
Justice Criminal Division, Child Exploitation and Obscenity Section	$4.38 million and 28 personnel allocated to combating child exploitation and obscenity offenses	The High Tech Investigative Unit deals with investigating any Internet medium that distributes child pornography, including peer-to-peer networks.
U.S. Customs Service CyberSmuggling Center	$15.6 million (over 144,000 hours) allocated to combating child exploitation and obscenity offenses[b]	The center is beginning to actively monitor peer-to-peer networks for child pornography, devoting one half-time investigator to this effort. As of December 16, 2002, the center had sent 21 peer-to-peer investigative leads to field offices for follow-up.

Source: GAO and agencies mentioned.

[a]Dollar amounts are approximate

[b]Customs was unable to separate the staff hours devoted or funds obligated to combating child pornography from those dedicated to combating child exploitation in general.

An important new resource to facilitate the identification of the victims of child pornographers is the National Child Victim Identification Program, run by the CyberSmuggling Center. This resource is 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 and from CyberTipline reports filed with NCMEC. It will initially hold over 100,000 images collected by federal law enforcement agencies from various sources, including old child pornography magazines.[22] 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

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

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, which became operational in January 2003,[23] is housed at the Customs CyberSmuggling Center and can be accessed remotely in "read only" format by the FBI, CEOS, the U.S. Postal Inspection Service, and NCMEC.

In summary, Mr. Chairman, our work shows that child pornography as well as adult pornography is widely available and accessible on peer-to-peer networks. Even more disturbing, we found that peer-to-peer searches using seemingly innocent terms that clearly would be of interest to children produced a high proportion of pornographic material, including some child pornography. The increase in reports of child pornography on peer-to-peer networks suggests that this problem is increasing. As a result, it will be important for law enforcement agencies to follow through on their plans to devote more resources to this technology and continue their efforts to develop effective strategies for addressing this problem.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other Members of the Committee may have at this time.

Contact and Acknowledgments

If you should have any questions about this testimony, please contact me at (202) 512-6240 or by E-mail at koontzl@gao.gov. Key contributors to this testimony were Barbara S. Collier, Mirko Dolak, James M. Lager, Neelaxi V. Lakhmani, James R. Sweetman, Jr., and Jessie Thomas.

[23] One 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.

Attachment: How File Sharing Works on 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, access to information and services is accomplished by interaction between clients—users who request services—and servers—providers of services, usually Web sites or portals. Unlike this 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.[24]

The ability of peer-to-peer networks to provide services and connect users directly has resulted in a large number[25] of powerful applications built around this model.[26] 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,[27] there are two main models of peer-to-peer networks: (1) the centralized model, in which a central server or broker directs traffic between individual registered users, and (2) the

[24] Matei 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)

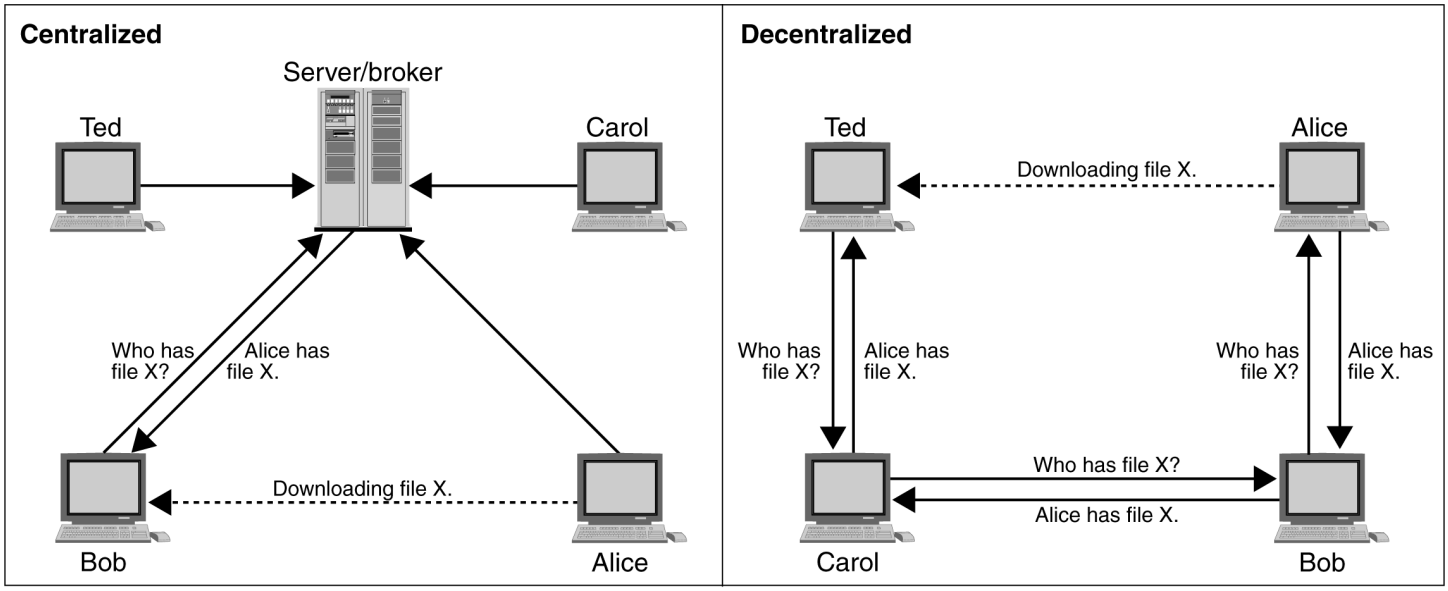
[25] Zeropaid.com, a file-sharing portal, lists 88 different peer-to-peer file-sharing programs available for download. (http://www.zeropaid.com/php/filesharing.php)

[26] Geoffrey 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)

[27] Illustration 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).

decentralized model, based on the Gnutella[28] network, in which individuals find each other and interact directly.

Figure 4: Peer-to-Peer Models



Source: Mark Bontrager, Bob Knighten.

As shown in figure 4, in the centralized model, a central server/broker maintains directories of shared files stored on the computers of registered users. When Bob submits a request for a particular file, the server/broker creates a list of files matching the search request by checking it against its database of files belonging to 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.

[28] According 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)

This broker model was used by Napster, the original peer-to-peer network, facilitating mass sharing of 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. Because much of this material was copyrighted, Napster as the broker of these exchanges was vulnerable to legal challenges,[29] which eventually led to its demise in September 2002.

In contrast to Napster, most current-generation peer-to-peer networks are decentralized. Because they do not depend on the server/broker that was the central feature of the Napster service, these networks are less vulnerable to litigation from copyright owners, as pointed out by Gartner.[30]

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 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; members will 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 can then open a connection with Alice and download the file directly from Alice's computer.[31]

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

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

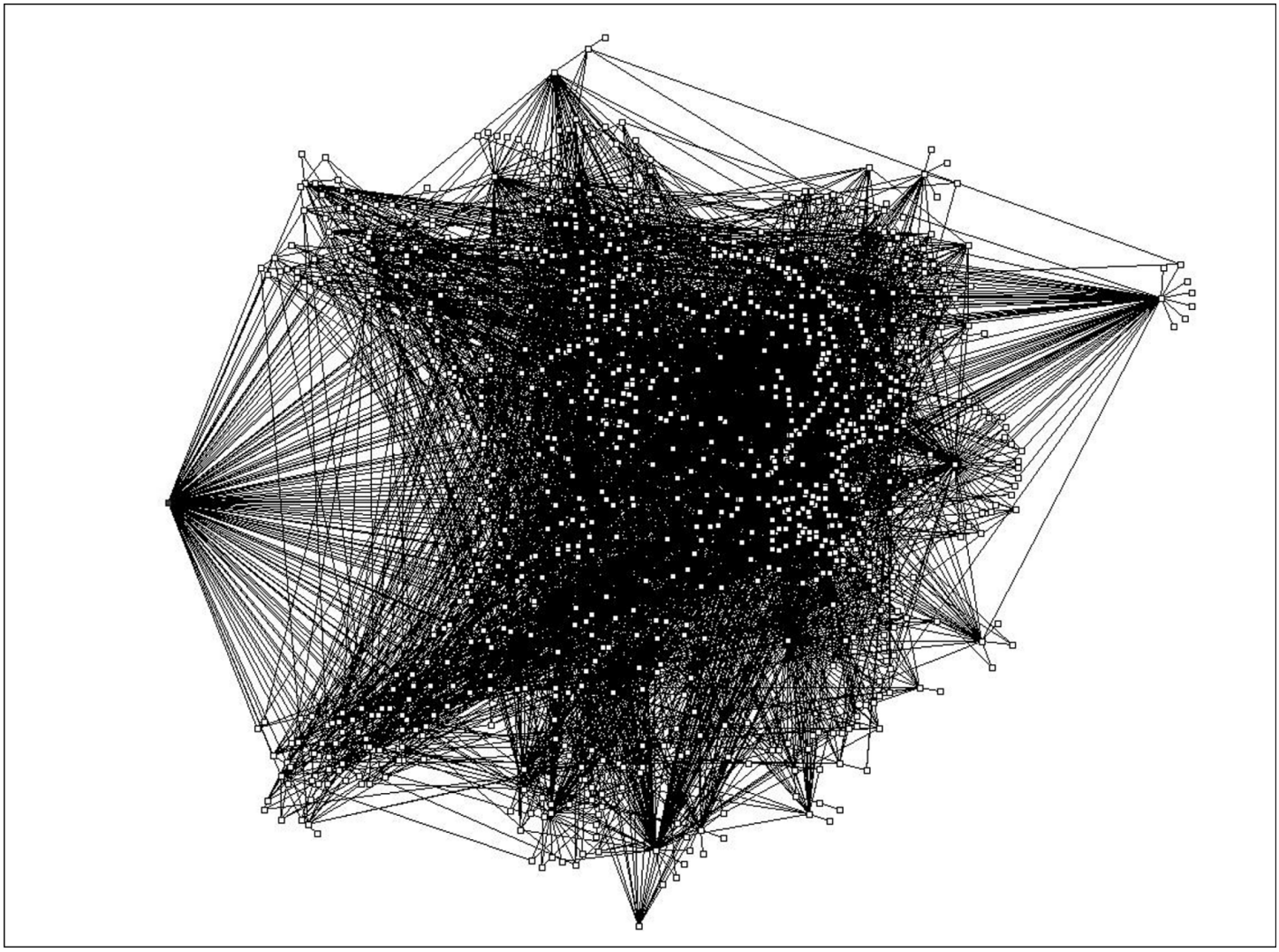
[30] Lydia Leong, "RIAA vs.Verizon, Implications for ISPs," Gartner (Oct. 24, 2002).

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

network visualization tool.[32] 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.

[32] Mihajlo 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.

One of the key features of many 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 using when they log on.[33] The VNS facilitates point-to-

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

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 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. Peer-to-peer users thus may appear to be anonymous; they are not, however. 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.