STUMBLING ONTO SMUT: THE ALARMING EASE OF ACCESS TO PORNOGRAPHY ON PEER-TO-PEER NETWORKS

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

MARCH 13, 2003

Serial No. 108–8

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE
87–066 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LaTOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, Jr., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

———

BERNARD SANDERS, Vermont (Independent)

Peter Sirh, *Staff Director*
Melissa Wojciak, *Deputy Staff Director*
Randy Kaplan, *Senior Counsel/Parliamentarian*
Teresa Austin, *Chief Clerk*
Philip M. Schiliro, *Minority Staff Director*

CONTENTS

STUMBLING ONTO SMUT: THE ALARMING EASE OF ACCESS TO PORNOGRAPHY ON PEER-TO-PEER NETWORKS

THURSDAY, MARCH 13, 2003

House of Representatives,
Committee on Government Reform,
Washington, DC.

The committee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis (chairman of the committee) presiding.

Present: Representatives Tom Davis, Waxman, Janklow, Miller, McHugh, Putnam, Tierney, Shays, Turner, Ruppersberger, Duncan, Kucinich, Cummings, Maloney, and Van Hollen.

Staff present: Peter Sirh, staff director; Melissa Wojciak, deputy staff director; Keith Ausbrook, chief counsel; Randall Kaplan, counsel; David Marin, director of communications; Scott Kopple, deputy director of communications; Drew Crockett, professional staff member; Teresa Austin, chief clerk; Joshua E. Gillespie, deputy clerk; Nancy Scola and David McMillen, minority professional staff members; and Jean Gosa, minority assistant clerk.

Chairman Tom Davis. Good morning, a quorum being present, the Committee on Government Reform will come to order. We are here today to examine a growing problem for parents across the country: the ease with which children can access pornography, including child pornography, through file sharing programs on peer-to-peer computer networks.

Peer-to-peer networks are Internet programs that allow users to access each other's computer files. Typically, people use these programs to share music, images, and video.

This technology is booming in popularity. At any given time, millions of people around the world are sharing their files. Napster, one of the first file sharing programs, had 1.6 million people exchanging music files, before being shut down by court order because of copyright violations.

Newer file sharing programs have become even more popular. KaZaA, one of the more popular networks, has been downloaded more than 199 million times, with 4 million users searching and sharing files at any given time.

Unlike Napster, these newer programs allow users to download videos and pictures, in addition to music files, and they do not operate through central servers. Without a central on-line hub acting as a filter, children can receive images and solicitations that normally would be blocked. In addition, the programs are easy to install, and the electronic files can be downloaded free of charge.

This leads us to the problem we are here to examine today. These networks have become an increasingly popular mechanism for the trafficking of very graphic pornography, including child pornography. We will hear startling testimony today about this problem.

At the request of Congressman Waxman and myself, the General Accounting Office conducted a study which found that child pornography is easily accessible on peer-to-peer networks.

Searches for child pornography by the GAO and the Customers Services on file sharing programs produced hundreds of pornographic images, more than half of which was child pornography and graphic adult pornography.

Also, research performed by MediaDefender, another of our witnesses, found that nearly 6 million pornography files were available for downloading on one popular peer-to-peer network in a recent 2-day period.

These findings are very disturbing, especially because file sharing programs are becoming increasingly popular with kids. Research has shown that more than 40 percent of the people who download files from file sharing programs are under the age of 18; and many of these pornographic images are appearing on our children's computer screens—whether they ask for it or not.

Seemingly innocent searches for files using the names of popular cartoon characters, singers, and actors produce thousands of graphic pornographic imagines, including child pornography.

I want to commend Congressman Waxman for bringing this important issue to our attention. We need to alert parents to this problem and discuss what they and we can do about it. Research performed by the committee staff has found that many of the tools available to parents to prevent access to pornography on peer-to-peer networks are ineffective. Many of the filtering devices within file sharing programs have limitations, as well.

So what is a parent to do? The current dynamic leaves parents in an untenable position; either watch over your child's shoulder every second while he or she is at the computer, or deny them use, or run the risk of exposure to this disgraceful material.

The alarming ease of inadvertent, unsolicited access to pornography on these networks threatens our children, period. We are not talking about bad language or simple bad taste. We are talking about ugly, graphic imagines that have no place in our homes, and that does not even include the child pornography that is just plain illegal.

Today we will be releasing two reports: one by the General Accounting Office and another committee staff report. These reports detail the problems of pornography on peer-to-peer networks and evaluate the effectiveness of parental control devices. I would like to thank all of our witnesses for appearing today, and I look forward to their testimony.

[The prepared statement of Chairman Tom Davis follows:]

TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS

Congreſs of the United States

Houſe of Repreſentatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY	(202) 225–5074
FACSIMILE	(202) 225–3974
MINORITY	(202) 225–5051
TTY	(202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT

Statement of Chairman Tom Davis
Government Reform Committee Hearing
"The Alarming Ease of Access to Pornography on Peer-to-Peer Networks"
March 13, 2003

We are here today to examine a growing problem for parents across the country: the ease with which children can access pornography, including child pornography, through file sharing programs on peer-to-peer computer networks.

Peer-to-peer networks are Internet programs that allow users to access each other's computer files. Typically, people use these programs to share music, images and video.

This technology is booming in popularity. At any given time, millions of people around the world are sharing their files. Napster, one of the first file sharing programs, had 1.6 million people exchanging music files, before being shut down by court order because of copyright violations.

Newer file sharing programs have become even more popular. Kazaa, one of the more popular networks, has been downloaded more than 199 million times with 4 million users searching and sharing files at any given time. Unlike Napster, these newer programs allow users to download videos and pictures, in addition to music files, and they don't operate through central servers. Without a central hub online to filter through, children can receive images and solicitations that normally would be blocked. In addition the programs are easy to install and the electronic files can be downloaded free of charge.

This leads us to the problems we are here to examine today. These networks have become an increasingly popular mechanism for the trafficking of very graphic pornography, including child pornography. We will hear startling testimony today about this problem. At the request of Congressman Waxman and myself, the General Accounting Office found that child pornography is easily accessible on peer-to-peer networks. Searches for child pornography by the GAO and the Customs Services on file sharing programs produced hundreds of pornographic images, more than half of which was child pornography and graphic adult pornography.

Also, research performed by MediaDefender, another of our witnesses, found that nearly six million pornographic files were available for downloading on one popular peer-to-peer network in a recent two-day period.

These findings are very disturbing, especially because file-sharing programs are becoming increasingly popular with kids. Research has shown that more than 40 percent of the people who download files from file sharing programs are under the age of 18. And many of these pornographic images are appearing on our children's computer screens -- ***whether they ask for it or not***. Seemingly innocent searches for files containing images of popular cartoon characters, singers and actors produce thousands of graphic pornographic images, including child pornography.

I want to commend Congressman Waxman for bringing this important issue to my attention. We need to alert parents to this problem and discuss what they – and we -- can do about it. Research performed by Committee staff has found that many of the tools available to parents to prevent access to pornography on peer-to-peer networks are ineffective. Also, many of the filtering devices within file sharing programs have limitations as well.

So, what's a parent to do? The current dynamic leaves parents in an untenable position: either watch over your child's shoulder every second he or she is at the computer, or deny them use, or run the risk of exposure to this disgraceful material.

The alarming ease of inadvertent, unsolicited access to pornography on these networks threatens our children. Period. We're not talking about bad language or simple bad taste – we're talking about ugly, graphic images that have no place in our homes. And that doesn't even include the child pornography that's just plain illegal.

Today we will be releasing two reports: one by the General Accounting Office and another Committee staff report. These reports detail the problem of pornography on peer-to-peer networks and evaluate the effectiveness of parental control devices. I would like to thank all of our witnesses for appearing today and I look forward to their testimony.

Chairman TOM DAVIS. I would now like to yield to Mr. Waxman for an opening statement. I understand that, Mr. Waxman, at the conclusion of our first set of witnesses, is going to walk us through a demonstration of how a file sharing program works, and how easy it is to access pornography using these programs. Mr. Waxman, thank you very much.

Mr. WAXMAN. Thank you, Mr. Chairman; I am pleased to join with you in this hearing today to draw attention to Internet technology that gives kids easy access to incredibly graphic pornography.

I am on the dias because I am a Congressman, but I do not want to speak as a public official. I want to speak as a parent and a grandparent. I want to speak about how difficult it is to raise a child today, and to raise some of these new issues that families must begin to consider.

We have two reports that we are issuing today on Internet file sharing programs: one from the General Accounting Office, and the other was prepared by our investigative staff.

What is in these reports should concern every parent in America. There is a new technology. It is widely available, and it allows teenagers to download "x" rated videos directly into their home computers. The most popular of these programs is KaZaA, which has been downloaded nearly 200 million times.

Other popular programs include Morpheus, BearShare, and Grokster. At any given time, there are millions of teenagers between the ages of 12 and 18 using these programs.

Now most adults I have talked to have never even heard of any of these file sharing programs. I certainly had never heard about it before it was brought to my attention by Robbie Barnett, whose father is the counsel on the Democratic side of this committee. He is our chief counsel of the Democratic side of the Government Reform Committee.

Robbie told his father about these Web sites, and I am pleased that Robbie is here to testify about it, before all of us. I am also pleased and want to welcome our chairman's daughter, Shelley, who is also going to be talking about this issue.

We are going to hear from both of them about how young people are being exposed to pornography that is being foisted upon them, as they go on to these file sharing sites.

I know that many people hear about these issues with regard to the entertainment industry, because they threaten copyrights, and I certainly care a lot about that issue, representing Hollywood.

But this hearing today is not about that issue. It is not about recording company profits or freedom on the Internet. It is about something more basic: how to raise children safely in today's digital age.

We ask the company, MediaDefender, to assess how much pornography is available to teenagers when they log on the Internet with KaZaA or other file sharing programs and what we learned was astounding. At any given time, as the chairman also mentioned, there are 6 million pornographic files available to kids to download. All of these files can be downloaded completely free of charge, directly to any computer that is connected to the Internet.

And if your child has access to a broadband connection, the most hard care, triple-x videos imaginable can be downloaded in just a few minutes.

Imagine if there was a library that held 6 million pornographic videos and magazines. No parent would allow their children to wander at will through its collections. But this is exactly what can happen every day, in millions of homes across American. Whenever a tech-savvy teenager logs on to programs like KaZaA, he or she has access to millions of hardcore pornographic files.

But it is even worse than this. As GAO has pointed out in their report, kids will be bombarded with pornography, even if they are not looking for it. GAO did searches for popular entertainment figures, like Britney Spears and the Olsen twins; and for cartoon characters like Pokemon.

What they found was that more than half of the files they retried were pornographic. In fact, they even retried files that contained illegal child pornography.

Now parents may think they are doing something about this problem, when they put in these parental control software programs, like Net Nanny or CyberPatrol. They think they can protect their children from this pornography.

But our investigation also found that while these programs might work to keep kids from pornography on the worldwide Web; they do not work in the same way for file sharing programs. There are some programs that can be configured, after some effort, to block access to all file sharing programs.

But there is really nothing that works effectively in filtering out pornographic files, once a child has access to these programs.

Now as legislators, we are always thinking about passing the law. But I am not sure there is a legislative solution to this program.

In this case, parental awareness, parental involvement matter more than legislation. Parents need to better understand these file sharing programs, and know if their kids are using them. Parents need to talk to their children about what to do when they come across this pornography. In short, we have to close the on-line generation gap.

To help parents meet this challenge, Chairman Davis and I have put together some straight-forward recommendations that we will be distributing today. These recommendations will also be available on our Web site.

I want to make clear that technical innovation on the Internet is tremendously important. When we discuss problems and challenges with computers in the Internet, we need to keep in mind that these technologies afford us many opportunities, and can be a great research to our children.

We should be aware that in trying to help children deal with the challenges of our times, we must not stifle the sort of innovations that have made the Internet and computers such powerful tools. But we also must make sure that the experiences on the Internet are safe ones.

I thank Chairman Davis for holding this hearing. It is an important one to get this issue out to people who otherwise might not know about it, which is probably the case for 90 percent of the parents in this country.

[The prepared statement of Hon. Henry A. Waxman follows:]

ONE HUNDRED EIGHTH CONGRESS

Congreſs of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY	(202) 225–5074
FACSIMILE	(202) 225–3974
MINORITY	(202) 225–5051
TTY	(202) 225–6852

www.house.gov/reform

Statement of Rep. Henry A. Waxman
Hearing on Stumbling into Smut: The Alarming Ease of Access to
Pornography on Peer-to-Peer Network
March 13, 2003

Today, I join with Chairman Tom Davis to draw attention to an Internet technology that gives kids easy access to incredibly graphic pornography.

I am on the dias today because I'm a congressman. But I do not want to speak as a public official. I want to speak as a parent and a grandparent. I want to speak about how difficult it is to raise a child today ... and to raise some new issues that families must begin to consider.

Today, Chairman Davis and I are releasing two reports on Internet file-sharing programs. One report is by the General Accounting Office, and one was prepared by our investigative staff.

What is in these reports should concern every parent in America. There's a new technology that's widely available that allows teenagers to download x-rated videos directly into their home computers.

The most popular of these programs is Kazaa, which has been downloaded nearly 200 million times. Other popular programs include Morpheus, BearShare, and Grokster. At any given time, there are millions of teenagers between the ages of 12 and 18 using these programs.

Most adults I talk with don't know about these programs. But if they do, all they know is that the entertainment industry doesn't like them because they threaten their copyrights.

This hearing is not about that issue. It's not about recording company profits or freedom of the Internet. It's about something more basic: how to raise children safely in today's digital age.

We asked a company, Media Defender, to assess how much pornography is available to teenagers when they log onto the Internet with Kazaa or other file-sharing programs. What we learned was astounding: at any given time, there are six million pornographic files available to kids to download. All of these files can be downloaded completely free of charge directly to any computer that's connected to the Internet.

And if your child has access to a broadband connection, the most hard-core, triple-x videos imaginable can be downloaded in just a matter of minutes.

Imagine if there was a library that held six million pornographic videos and magazines. No parent would allow their child to wander at will through its collections.

But this is exactly what can happen every day in millions of homes across America. Whenever a tech-savvy teenagers log on to programs like Kazaa, he or she has access to millions of hard-core pornographic files.

But it's even worse than this. As GAO's investigation found, kids will be bombarded with pornography even if they aren't looking for it. GAO did searches for popular entertainment figures like Britney Spears and the Olson Twins and for cartoon characters like Pokemon. And what they found was that more than half of the files they retreived were pornographic. In fact, they even retrieved files that contained illegal child pornography.

Parents may think that by installing parental control software programs like Net Nanny or Cyber Patrol, they can protect their children from this pornography. But our investigation also found that while these programs might work to keep kids from pornography on the World Wide Web, they do not work in the same way for file-sharing programs. There are some programs that can be configured – after some effort – to block access to all file-sharing programs. But there's really nothing that works effectively in filtering out pornographic files once a child has access to these programs.

As legislators, we can try to pass laws. But I'm not sure there's a legislative solution available for this problem. In this case, parental awareness and parental involvement matter more than legislation. Parents need to better understand these file-sharing programs and know if their kids are using them. Parents need to talk to their children about what to do when they come across this pornography.

In short, we have to close the online generation gap.

To help parents meet this challenge, Chairman Davis and I have put together some straightforward recommendations that we will be distributing today. These recommendations will also be available on our websites.

I want to make clear that technical innovation on the Internet is tremendously important. When we discuss problems and challenges with computers and the Internet, we need to keep in mind that these technologies afford us many opportunities and can be great resource for our children. We should be aware that in trying to help children to deal with the challenges of our times we must not stifle the sort of innovations that have made the Internet and computers such powerful tools.

But we also must make sure that their experiences on the Internet are safe ones.

As part of helping parents learn more about these programs, we have arranged for a demonstration of how these programs work. Before we start this demonstration, I want to warn the members and audience that even the names of the files can contain be offensive and pornographic. We're going to show the unredacted names on the screens in the room because that's what our children are actually seeing. But we also have posters up that display the results in a redacted form for those who find this less offensive.

Chairman TOM DAVIS. Mr. Waxman, thank you very much; and thank you very much for your leadership on this.

Are there any other opening statements? Mr. Janklow.

Mr. JANKLOW. Mr. Chairman, thank you very, very much for convening this particular hearing. Mr. Chairman, in my previous capacity as Governor of South Dakota, we convened the first Statewide conference in the Nation, back in 2001, to deal with this issue.

Let me, if I can, give you some additional statistics to add to what it is; and material that you and Mr. Waxman so graciously have provided.

We all know that if you go to whitehouse.com, you are going to get the wrong thing. You are going to get a pornography site. Parents cannot deal with this. Parents cannot fix this. These are accidental things.

If you go to playstation.com, you are going to get a kids' station. If you make a mistake and hit an "m" instead of an "n". You are going to go a pornographic site.

So if you to crazyhorse.org, you are going to get the Crazy Horse memorial. If you go to crazyhorse.com, you are going to get a pornographic site.

These pornographic sites have cookies in them, which then make it so that you cannot get them off your screen. The more you try and delete them, they more they are added to the scenery.

As a matter of fact, back in 2001, the Federal Trade Commission, in 2 weeks, shut down 5,500 sites that were called copycat sites, where people were able to mistakenly get onto these things.

You talk about the cartoon network. If you hit cartoonnetwork.com and make a mistake in the spelling, there are 15 different derivatives of that, that will give you a pornographic site for children that they cannot get off of their computers.

There are 41 variations of Britney Spears' spelling. Only the accurate spelling of Britney Spears will get you into a good site. All the rest of them will get you into a pornographic site, that children will get their hands on.

If you talk about how many sites there are, in 2001, according to google.com, there were 1.4 billion registered domains; 168 million, approximately 12 percent were pornographic sites; 12 percent of 1.4 billionsites. That is about 168 million pornographic sites in the world for children.

According to a study done by the University of New Hampshire of students age 10 to 17, 20 percent of these students that were surveyed by the University of New Hampshire, these students had received unwanted sexual solicitations during the previous year.

Three percent had been actually asked to meet off line, had been called on the telephone, or sent money or gifts by a male, which are called aggressive solicitations.

Also, according to that survey, 97 percent of the solicitors were strangers; but something more important, only 10 percent of the students indicated that they had ever told their parents or teachers about having been contacted on these sites.

In addition to that, the sexual solicitations, one of the things we have to recognize, we all argue about the first amendment. Seventy percent of these solicitations of these students, according to the

University of New Hampshire's survey, were done at home. They were not done in school and they were not done in libraries.

But I also submit, Mr. Chairman, the first amendment was never written to take care of predators. It was never written to allow anybody to prey on our children.

Also, if you look at what we need to do, we need to do something, in a legislative sense, to get these people away from computers, to scoop them off the street. Where we have mountain lions that attack people, where we have grizzly bears that attack people, we deal with them.

These predators are worse than an animal. An animal will just kill you. These predators will prey on people and destroy them as human beings.

So Mr. Chairman, I thank you for convening this meeting. This is something that is incredibly important, and it is a far bigger problem than any of us can imagine. You stumble onto these sites. You cannot get off of them.

Once children start being subjected to these kinds of things, it is a very, very quick maneuver to get them to the point where they continue moving forward with it. Thank you very much.

Chairman TOM DAVIS. Thank you very much; well, if there are no other statements, will move to our first panel of witnesses. We have Shelley, a 9th grader, and Robert, a 10th grader, who will discuss their experiences with these file sharing programs.

It is the committee's policy, the ladies go first, Robert; so Shelley?

STATEMENT OF MISTRESS SHELLEY, NINTH GRADE, AND MASTER ROB, TENTH GRADE

Mistress SHELLEY. Mr. Chairman, Ranking Member Waxman, and members of the committee, thank you for allowing me to be here today to discuss problems related with Internet file sharing programs.

I am a 15 year old ninth grader from Falls Church, VA. Kids my age across the country are using file sharing programs to retrieve a variety of items. I, personally, have many friends who use programs like KaZaA and Grokster.

These programs are easily accessible and not complicated. All you do is log onto the Internet, go to the program Web site, and download the program, which does not take very long.

Once you have the program on your computer, it is very simple to search and share files; and the file sharing is free of charge and downloads in a matter of seconds.

Many of my friends use programs like KaZaA. When they search for materials by specific singers or actors, they are often surprised with their results. For example, when you type in Britney Spears, some files with her name come up. However, some of the file names that come up contain pornographic language; language that I would rather not repeat before the committee.

The vast majority of files that appear have pornographic language and, if downloaded, become visuals. Most of the descriptions suggest that the file is not related to the search, Britney Spears, at all.

My friends are very uncomfortable and apprehensive about using these programs. They can be very scary. Minimal effort is required to find this kind of pornography. Among teenagers and kids, this is a widespread situation.

Although this is a big problem for kids my age, my main concern is for the younger children. You have to work very, very hard not to get pornography when you use these programs. Without proper parental supervision, young kids can be exposed to this harmful material at a very young age.

I thank you for allowing me to give my views on this very important topic, and hope you take my words into consideration, thank you.

[The prepared statement of Mistress Shelley follows:]

Mr. Chairman, Ranking Member Waxman, and members of the Committee, thank you for allowing me to be here today to discuss problems related with Internet file sharing programs. I am a 15 year old, ninth grader from Falls Church, Virginia.

Kids my age across the country are using file-sharing programs to retrieve access to a variety of stuff. I personally have many friends who use programs like Kazaa and Grokster. These programs are easily accessible and not complicated. All you do is log onto the Internet, go to the program website, and download the program, which doesn't take very long.

Once you have the program on your computer, it is very easy to search and share files. And the file sharing is free of charge and downloads in a matter of seconds.

Many of my friends use programs like Kazaa. When they search for materials by specific singers or actors they are often very surprised with the results. For example, when you type in "Britney Spears," *some* files with her name, come up.

However, some of the file names that come up contain pornographic language – language that I would rather not repeat before this Committee. The vast majority of files that appear have pornographic language, and if downloaded, become visuals. Most of the descriptions suggest that the file is not related to the search, Britney Spears at all.

My friends are very uncomfortable and apprehensive about using these programs. It can be very scary. Minimal effort is required to find this kind of pornography. Among teenagers and kids, this is a wide spread situation.

Although this is a big problem for kids my age, my main concern is for the younger children. You almost have to work very hard NOT to get pornography when you use these programs. Without proper parental supervision, young kids can be exposed to this harmful stuff at a very young age.

I thank you for allowing me to give my views on this very important topic, and hope you take my words into consideration. Thank you.

Chairman TOM DAVIS. Thank you very much.

Rob, thanks for being with us.

Master ROB. Good morning and thank you, Mr. Chairman, Congressman Waxman, and the rest of the Members here today. I am here to share with you a kids' perspective on file sharing programs.

In the past few years, the popularity of file sharing programs has increased dramatically. A major group of users consists of high school students, such as myself, and it is not hard to see why.

Rather than spending $16, $18, or even $20 on a CD, any teenager with access to the Internet can type in a few words and download any song, free of charge. This simple action saves both time and money. Unfortunately, there are many problems with these file sharing programs.

I know that record companies worry about copyright issues, but most kids are not too concerned about that. A real problem, though, is the fact that file sharing programs provide easy access to illegal pornography.

Even worse, much of this pornography is deceptively shared under the names of popular singers or actors. A child searching for a song or a movie is likely to stumble upon imagines or videos of a pornographic nature. Most people using file sharing programs have probably stumbled upon pornographic files at one time or another.

Even if your computer has a parental control program installed, it probably will not work. For the most part, file sharing programs go unnoticed, both by parental control programs and by parents themselves.

Most kids are aware of these problems, and have learned to deal with them by filtering their searches or skipping over pornographic material. However, many parents do not realize the prevalence of pornography on file sharing programs, and are understandably surprised when they learn that their teenager may have been exposed to inappropriate material.

It is important that we bring this issue into the public conscience, so that parents can discuss these issues with their teenagers. In order to protect teens from viewing illicit material, the ease of access to pornography on file sharing networks must be addressed; thank you.

[The prepared statement of Master Rob follows:]

Good morning, and thank you Mr. Chairman, Congressman Waxman, and the rest of the members here today. I am here to share with you a kid's perspective on file-sharing programs. In the past few years, the popularity of file-sharing programs has increased dramatically.

A major group of users consists of high-school students such as myself, and it's not hard to see why. Rather than spending 16, 18, or even 20 dollars on a CD, any teenager with access to the internet can type in a few words and download any song free of charge. This simple action saves both time and money. Unfortunately, there are many problems with these file-sharing programs.

I know that record companies worry about copyright issue, but most kids aren't too concerned about that. A real problem, though, is the fact that file-sharing programs provide illegal access to illegal pornography. Even worse, much of this pornography is deceptively shared under the names of popular singers or actors. A child searching for a song or movie is likely to stumble upon images or videos of a pornographic nature. Most people using file-sharing programs have probably stumbled on pornographic files at one time or another.

Even if your computer has a parental control program installed, it probably won't work. For the most part, file sharing programs go unnoticed, both by parental control programs and by parents themselves.

Most kids are aware of these problems and have learned to deal with them by filtering their searches or skipping over pornographic material. However, many parents do not realize the prevalence of pornography on file-sharing programs and are understandably surprised when they learn that their teenager may have been exposed to inappropriate material. It is important that we bring this issue into the public conscience, so that parents can discuss these issues with their teenagers. In order to protect teens from viewing illicit material, the ease of access to pornography on file-sharing networks must be addressed. Thank You.

Robert Barnett

Chairman TOM DAVIS. Well, thank you very much. I know you are both eager to get back to school. [Laughter.]

Let me just ask each of you, do you think more parental supervision is needed when kids are using these services?

Mistress SHELLEY. Yes, I do. Parents need to be aware and more involved with their child's use of the Internet, especially file sharing software.

Chairman TOM DAVIS. Rob.

Master ROB. I do. It is important that parents are aware of this problem, and that they watch their kids, to make sure that their kids are not looking at anything they should not be looking at.

Chairman TOM DAVIS. Well, let me just say for the record, I just only became aware of the nature of the seriousness of this as we were preparing for this hearing. I would just say, as a concerned parent, I want to do everything I can to remove the file sharing from computers that our kids use.

This is really very alarming to me, as a parent who thought he was tech-savvy on this kind of thing, to see how far this has gone.

Mr. Waxman, do you have some questions?

Mr. WAXMAN. Well, thank you, Mr. Chairman; and thank you both for your testimony. We often hear from witnesses who have represented different organizations or trade associations or economic interests. They come in with their prepared testimony, screened by their lawyers and very carefully calculated, and they get some legislation across.

But the two of you have given us a perspective that we do not usually see, and that is from two young people, who know more about using the Internet than most adults.

Let me just ask you a technical question, because parents get these screening mechanisms to stop their kids from going on certain Internet sites.

What is the difference between the Internet site and file sharing? Will those filters not stop any transmission of pornography to a young person on the Internet? Rob, do you want to talk about that?

Master ROB. Well, the filters are designed to stop the Internet sites. Since this problem on file sharing programs is relatively new and they have not been around for too long, the programs probably are not designed to handle these kind of programs.

Mr. WAXMAN. So if a parent bought software to put in to block their kids from getting any pornography off an Internet site; for instance, our colleague, Mr. Janklow, went to a number of Internet sites that might lead to pornography; so parents could block those.

But if the kids were using file sharing to get music, they get bombarded with pornography and that is not blocked. Is that what you are telling us?

Master ROB. Yes, most programs do not block these file sharing programs. I am sure some do, but not all of them.

Mr. WAXMAN. Shelley, most of us have never heard about this problem. I did recently, but for most of us, it has been very, very recent.

Do most of your friends, most of the kids in school, know about all of this?

Mistress SHELLEY. Yes, I was one of the last actually, of my friends, to know about this. All my friends have been doing it for quite some time. [Laughter.]

Mr. WAXMAN. And did you tell your parents immediately? [Laughter.]

Chairman TOM DAVIS. I think it was last night. I think I can say that, because I was telling her about the hearing. [Laughter.]

Mr. WAXMAN. Well, I think it is important for parents to know. They think they know a lot, but kids know things that we never even imagined, and that is why we have to, as parents, and in my case, grandparent, talk to our youngsters about what is going on; what is new; and try to search what they are being exposed to that we never would have even imagined, such a short time ago.

Thank you, Mr. Chairman, and I thank you both of you for being here.

Chairman TOM DAVIS. Thank you very much.

I know they need to get back, but Mr. Shays, I know you wanted to ask one quick question.

Mr. SHAYS. Yes, I have just a very quick question.

I voted against, and I probably made a mistake, the whole issue of the V-chip, as it related to TV. This is designed so that parents can make sure their kids do not watch certain TV programs. But my logic was that the parent had to ask the child how to set the TV, so that the kid could not watch it.

I want to ask you, Shelley, do you think that young people know the Internet and know tech issues better than their parents?

Mistress SHELLEY. Yes. [Laughter.]

Definitely; I am always helping my mom or dad with the computer. So if there was a program that they had to set up for their children, their children would be the ones setting it up, in most cases.

Chairman TOM DAVIS. Chris, we are going somewhere I do not think we need to go. [Laughter.]

Mr. SHAYS. Thank you; I have no more questions.

Chairman TOM DAVIS. Thank you; we are going to do a demonstration now with Mr. Waxman, and I am going to ask the witnesses to leave the room. But let me just say to both of you, thank you very much. You have contributed a lot to our understanding of this; thank you very much.

[Applause.]

Chairman TOM DAVIS. Mr. Waxman.

Mr. WAXMAN. Well, Mr. Chairman, as part of helping parents learn more about these programs, we have arranged for a demonstration of how these programs work.

Before we start this demonstration, I want to warn the members and the audience that even the names of the files can contain offensive and pornographic images.

We are going to show the unredacted names on the screens in the room, because that is what our children are actually seeing. But we also have posters up that display the results in a redacted form, for those who find this less offensive.

So without viewing the sites themselves, let us just see what kids see when they have this pornography pushed upon them.

Ms. SCOLA. Thank you, Chairman Davis and Congressman Waxman. I am going to be showing you today how easy it is to download these file sharing programs and to use them. The most popular of these programs is KaZaA, and I will be downloading that program.

You can just go to any Internet browser, as long as you have an Internet connection set up. Go to a search engine and type in KaZaA. The first site pops up. Click on it. That brings you to the KaZaA Web site. Click on download now. This is free software. It requires no personal information.

Since we are on a dial-up connection here today, I am going to skip over the actual download part. It would take too long.

Once the software is installed on your desktop, you double click. That brings up a search field. You type in, let us say, Britney Spears, and it will search for images of Britney Spears. Veryquickly, this is what you get.

I know it is difficult to see, so we did some searches yesterday. I am going to zoom in on the results. These are the first several results you get for searching for Britney Spears.

If you search for Olsen twins, teenage actresses, this is what you get; and if you search for Pokemon, the cartoon character, this is what you get.

Chairman TOM DAVIS. The graphics are far worse, I assume. The graphics then that you get when you download are far worse, the language.

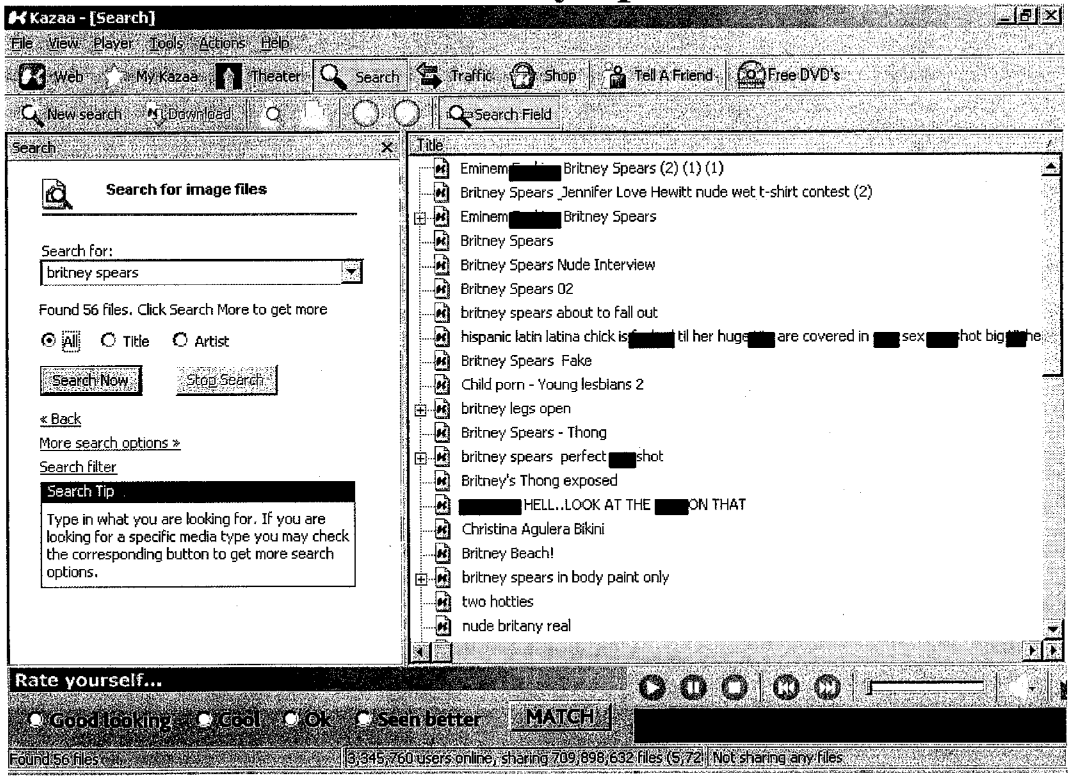
Ms. SCOLA. Yes.

Mr. WAXMAN. Well, Mr. Chairman, what we see is a menu then offered that, just looking at the titles of the menu, is pretty disgusting, in and of itself. But if you then clicked on any of these items, kids would immediately be led to a pornographic site.

I want to thank Nancy Scola, who is a professional staff member from the committee, who has worked on this investigation and other investigations for her presentation to us. It illustrates how simple it is, and how readily available it is for kids who might admire Britney Spears to be led to be confronted with a pretty raw kind of pornography.

[The information referred to follows:]

Search Results for “Britney Spears”



Search for image files

Search for:
britney spears

Found 56 files. Click Search More to get more

● All ○ Title ○ Artist

Search Now   Stop Search

« Back
More search options »
Search filter

Search Tip

Type in what you are looking for. If you are looking for a specific media type you may check the corresponding button to get more search options.

Eminem[redacted]Britney Spears (2) (1) (1)
Britney Spears _Jennifer Love Hewitt nude wet t-shirt contest (2)
Eminem[redacted]Britney Spears
Britney Spears
Britney Spears Nude Interview
Britney Spears 02
britney spears about to fall out
hispanic latin latina chick is[redacted] til her hug[redacted] are covered in [redacted] sex[redacted]hot big[redacted]he
Britney Spears Fake
Child porn - Young lesbians 2
britney legs open
Britney Spears - Thong
britney spears perfect [redacted]shot
Britney's Thong exposed
[redacted]HELL..LOOK AT THE [redacted]ON THAT
Christina Agulera Bikini
Britney Beach!
britney spears in body paint only
two hotties
nude britany real

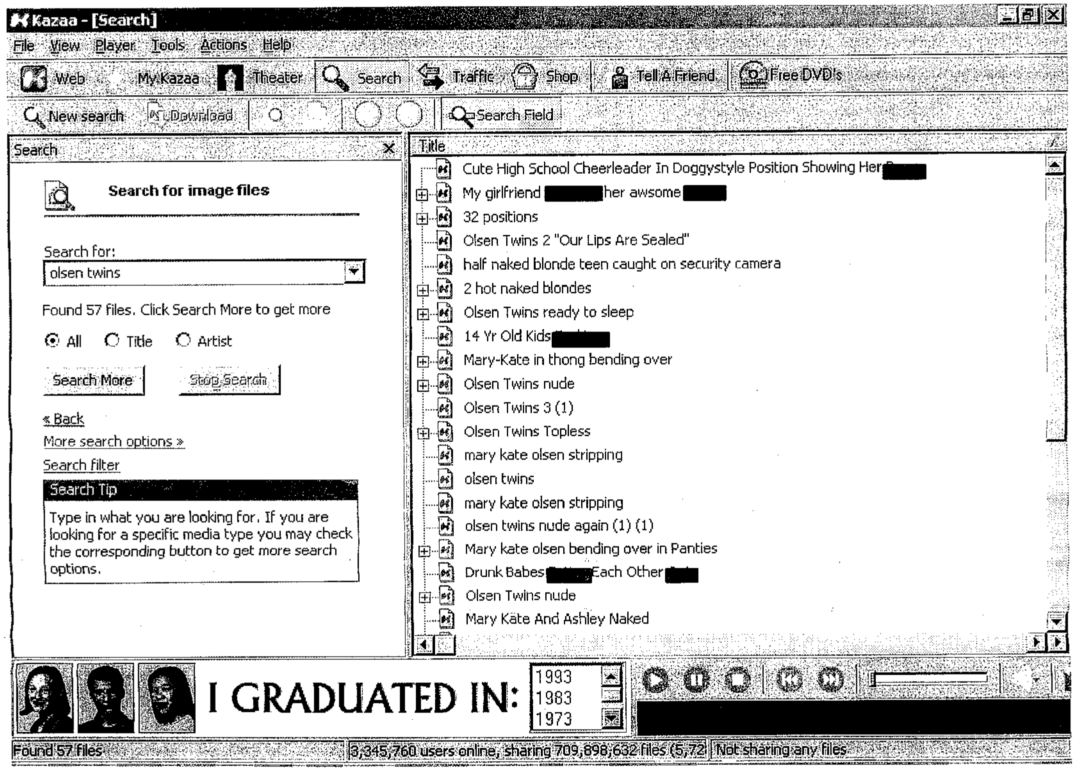
Rate yourself...

○ Good looking ○ Cool ○ Ok ○ Seen better   MATCH

[redacted]

Found 56 files | 3,345,760 users online, sharing 709,898,632 files (5,72 | Not sharing any files

Search Results for "Olsen twins"



Search for: olsen twins

Found 57 files. Click Search More to get more

● All ○ Title ○ Artist

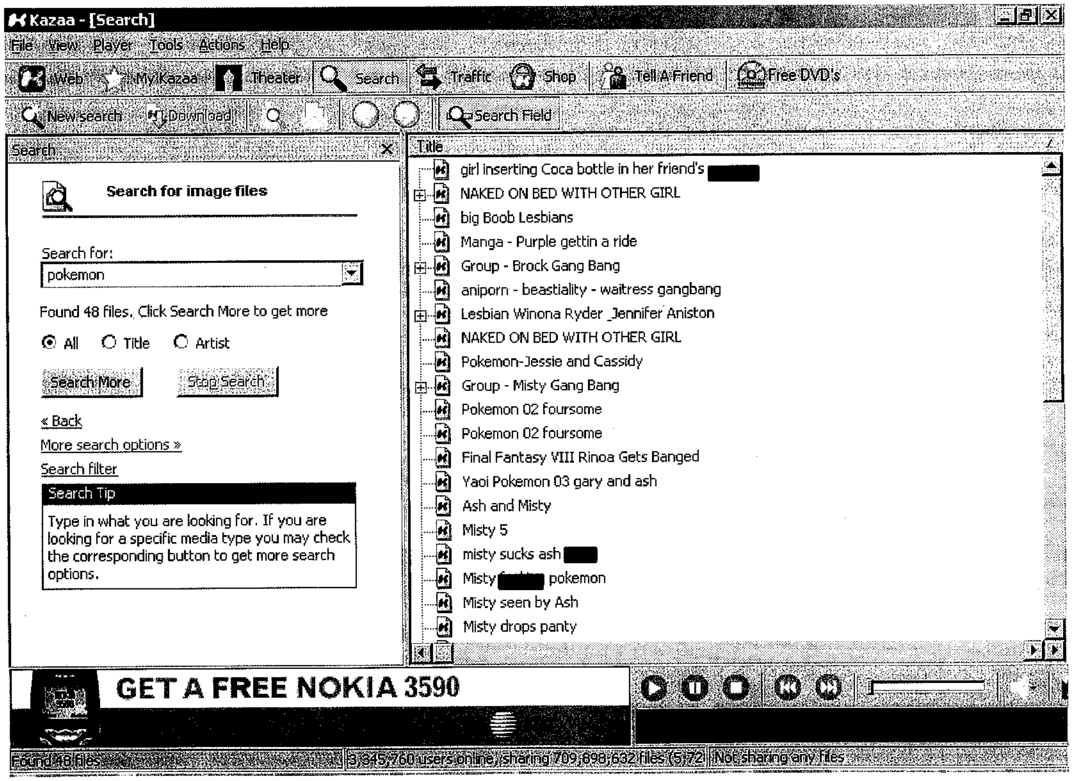
Type in what you are looking for. If you are looking for a specific media type you may check the corresponding button to get more search options.

Title

- Cute High School Cheerleader In Doggystyle Position Showing Her[redacted]
- My girlfriend [redacted]her awsome[redacted]
- 32 positions
- Olsen Twins 2 "Our Lips Are Sealed"
- half naked blonde teen caught on security camera
- 2 hot naked blondes
- Olsen Twins ready to sleep
- 14 Yr Old Kids[redacted]
- Mary-Kate in thong bending over
- Olsen Twins nude
- Olsen Twins 3 (1)
- Olsen Twins Topless
- mary kate olsen stripping
- olsen twins
- mary kate olsen stripping
- olsen twins nude again (1) (1)
- Mary kate olsen bending over in Panties
- Drunk Babes[redacted]Each Other[redacted]
- Olsen Twins nude
- Mary Kate And Ashley Naked

Found 57 files | 3,345,760 users online, sharing 709,898,632 files (5,72 | Not sharing any files

Search Results for “Pokemon”



Kazaa - [Search]
File View Player Tools Actions Help
Web My Kazaa Theater Search Traffic Shop Tell A Friend Free DVD's
New search Download Search Field
Search
Title

Search for image files

Search for: pokemon

Found 48 files. Click Search More to get more

● All ○ Title ○ Artist

Search More Stop Search

« Back

More search options »

Search filter

Search Tip

Type in what you are looking for. If you are looking for a specific media type you may check the corresponding button to get more search options.

- girl inserting Coca bottle in her friend's [redacted]
- NAKED ON BED WITH OTHER GIRL
- big Boob Lesbians
- Manga - Purple gettin a ride
- Group - Brock Gang Bang
- aniporn - beastiality - waitress gangbang
- Lesbian Winona Ryder _Jennifer Aniston
- NAKED ON BED WITH OTHER GIRL
- Pokemon-Jessie and Cassidy
- Group - Misty Gang Bang
- Pokemon 02 foursome
- Pokemon 02 foursome
- Final Fantasy VIII Rinoa Gets Banged
- Yaoi Pokemon 03 gary and ash
- Ash and Misty
- Misty 5
- misty sucks ash [redacted]
- Misty [redacted] pokemon
- Misty seen by Ash
- Misty drops panty

GET A FREE NOKIA 3590

Found 48 files | 3,345,760 users online, sharing 709,898,632 files (5,72 | Not sharing any files

Chairman TOM DAVIS. Mr. Waxman, let me also say, my understanding, in talking to some of the kids that use this is, some of the things that appear innocuous, in terms of their description when you download them are, in fact, way over the line. There is no warning whatsoever. They think they are downloading something that is decent and it is not; so thank you very much.

Let me move to our second panel now. I would like to thank our witnesses for appearing today. We have Linda Koontz from the General Accounting Office; John Netherland, from the Department of Homeland Security's Bureau of Immigration and Customs Enforcement; Randy Saaf, of MediaDefender; Daniel Rung from the file sharing company, Grokster; and Dr. Patricia Greenfield from UCLA's Department of Psychology.

It is the policy of the committee that all witnesses be sworn before they testify. If you will just stand with me and raise your right hands.

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you all for being here with us today. In order to allow time for more questions and discussion, if you could limit your testimony to 5 minutes. Your written statements are going to be in the record.

I think, for the most part, we have read the statements, and we already have some questions in mind. But it would be helpful, I think, for everybody to take about 5 minutes and sum up.

You have a light there in front that when the green is on, you keep going; when it is orange, that means you have a minute to sum up; and when it is red, your 5 minutes are up, if you could try to sum up. That way, we can get through it quickly and get to the questions.

Thank you very much, and let us start with Ms. Koontz. Thank you very much for being here.

STATEMENTS OF LINDA KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GENERAL ACCOUNTING OFFICE; JOHN M. NETHERLAND, ACTING DIRECTOR, CYBERSMUGGLING CENTER, BUREAU OF IMMIGRATION AND CUSTOMS ENFORCEMENT, DEPARTMENT OF HOMELAND SECURITY; RANDY SAAF, PRESIDENT, MEDIADEFENDER, INC.; DANIEL RUNG, CHIEF EXECUTIVE OFFICER, GROKSTER, LTD.; AND PATRICIA GREENFIELD, DEPARTMENT OF PSYCHOLOGY, UNIVERSITY OF CALIFORNIA AT LOS ANGELES

Ms. KOONTZ. Mr. Chairman, members of the committee, thank you very much for having us here to discuss the results of our work on the availability of child pornography on peer-to-peer networks. We have provided the results of our work to you today in a report that is being released.

To summarize, I would like to provide a little more background on peer-to-peer networks, and also discuss the ease of access to child pornography and peer-to-peer networks; the risk of inadvertent exposure of juvenile users to pornography; including child pornography on these networks; and the extent of Federal law enforcement resources available for this effort.

To build a little bit on what we have discussed earlier, our first chart shows the two main types of peer-to-peer networks. On the left, it shows the centralized network, where there is a central server or broker that maintains a directory of all the shared files that the users have, and directs traffic between those users.

The centralized model was employed by Napster, which was the original peer-to-peer network. Because much of the material traded on that network was copyrighted, Napster, as the broker of these exchanges, was vulnerable to legal challenge, and this eventually led to their demise late last year.

On the right side of the chart, we had the de-centralized model, which is what the most popular peer-to-peer networks are now using. In this model, the users are enabled to directly locate each other and interact.

On our next slide, we found that child pornography, as well as other types of pornography, are widely available and accessible through peer-to-peer networks. We use KaZaA, a very popular file sharing program to search for image files using 12 key words that are known to be associated with child pornography on the Internet.

As shown in our chart of over 1,200 items we identified, about 42 percent of the file names were associated with child pornography, and about 34 percent were associated with adult pornography.

On the next slide, we show another KaZaA search, where we worked with the Customs CyberSmuggling Center, to use three key words to search for and download child pornography images.

As you can see on this chart, this search identified 341 files, and about 44 percent of these were classified as child pornography, and about 29 percent as adult pornography.

I think more disturbing, however, was that we found that there is a significant risk that juvenile users of peer-to-peer networks can be inadvertently exposed to pornography, including child pornography in using these networks.

In searches, again, on KaZaA, using three innocuous search terms, that would likely be used by juveniles, we found that of the files that were returned, almost 50 percent of them were pornography, including a small amount of child pornography.

In regard to resources, we were not able to specifically quantify the amount of law enforcement resources that are devoted to peer-to-peer networks, because largely Federal law enforcement agencies do not track their resources by the specific Internet technologies.

However, these agencies indicated that as the tips are increasing in this area, they are increasing their efforts and their resources that are allocated to it.

That concludes my statement. I would be happy to answer questions at the end of the panel.

[The prepared statement of Ms. Koontz follows:]

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
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

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.

March 2003

FILE-SHARING PROGRAMS

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

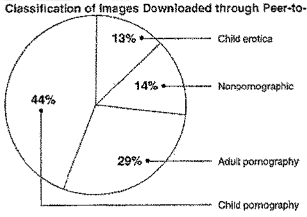
What GAO Found

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 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 child pornography on the Internet.[3] Of 1,286 items

[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.

[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.

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.

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

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

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

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

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.

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

[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.

[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)

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).

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.

[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.

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. 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]

[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*, National Academy Press (Washington; D.C.: 2002). (http://www.nap.edu/html/youth_internet/)

[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)

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 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]

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

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

[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.

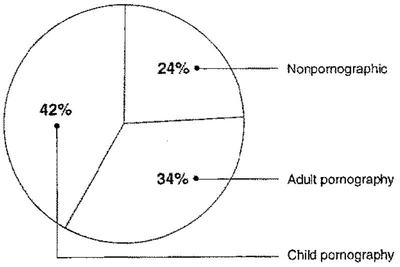
newsgroups, chat rooms, or the computers of users of peer-to-peer networks. The center also investigates leads from Internet service providers via the Exploited Child Unit's CyberTipline II.

- 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.

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.

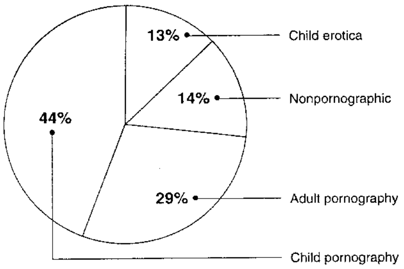
[20] The 12 keywords were provided by the Cybersmuggling Center as examples known to be associated with child pornography on the Internet.

[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.

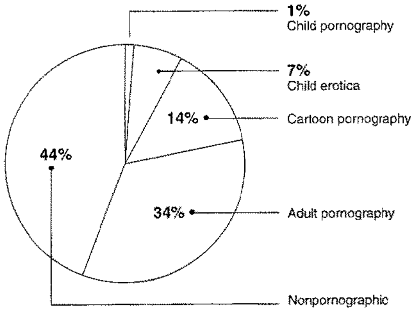
Juvenile Users of Peer-to-Peer Applications May Be Inadvertently Exposed to Pornography

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.

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. 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 is 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 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.

[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.

[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.

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

Contact and Acknowledgements

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.

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

[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)

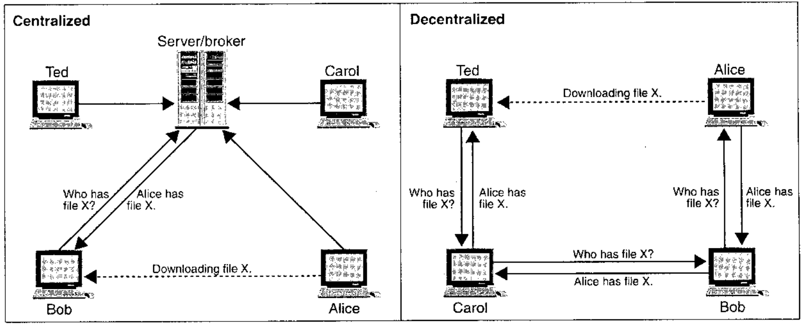
[25] Zeropaid.com, a file-sharing portal, lists 88 different peer-to-peer file-sharing programs available for download. (http://www.zeropaid.com/php/filesharing.php)

[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).

[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)

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, 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.

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

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

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; each member 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]

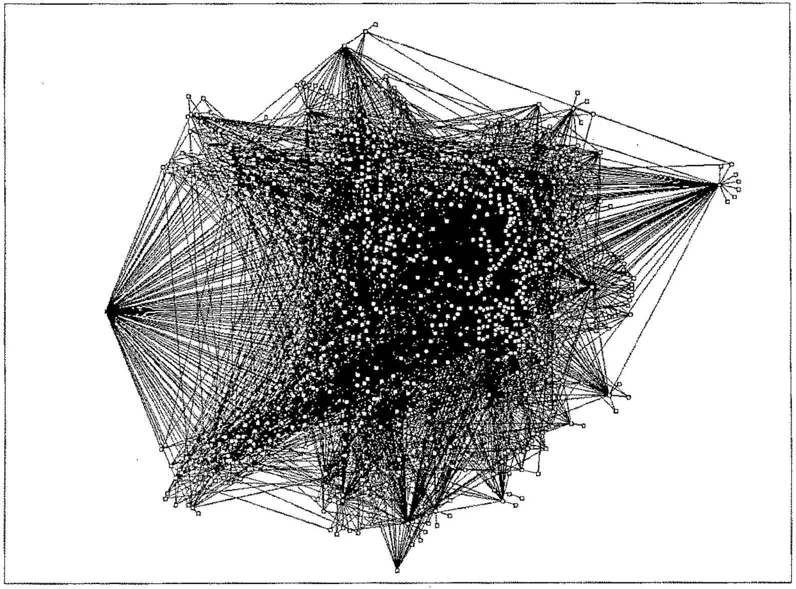
The file-sharing networks that result from the use of peer-to-peer technology are both extensive and complex. Figure 5 shows a map or topology of a Gnutella network whose connections were mapped by a network visualization tool.[32] The map, created in December 2000, shows 1,026 nodes (computers connected 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.

[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)

[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-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

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

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.

(310365)

Chairman TOM DAVIS. Thank you very much.

Mr. Netherland.

Mr. NETHERLAND. Mr. Chairman and distinguished members of the committee, it is a privilege to appear before you today to discuss the CyberSmuggling Center's efforts to investigate child exploitation that is facilitated by the Internet.

The CyberSmuggling Center, led by the Bureau of Immigration and Customs Enforcement, will continue to combat the sexual exploitation of children and the unfettered accessibility and illegal bartering of child pornography on the Internet via peer-to-peer file sharing networks.

The peer-to-peer file sharing networks are but one more means by which pedophile predators ply their trade and victimize our children; and the CyberSmuggling Center is expanding its investigative efforts to encompass this new technology.

The CyberSmuggling Center, located in Fairfax, VA, is recognized both nationally and internationally as a leader in the area of child exploitation investigations. The CyberSmuggling Center utilizes its resources and cutting edge technology as a means to protect our Nation's children from sexual abuse.

We have had a number of great successes in identifying and apprehending pedophiles. Recent investigative successes include: Operation HAMLET, a global investigation that resulted in the complete dismantlement of a ring of pedophiles who were molesting their own children and posting the images on the Internet for worldwide consumption. Many of these pedophiles were parents.

The CyberSmuggling Center, in its coordinating role, identified and rescued more than 100 children who were subjected to this torturous environment. The majority of these children were American citizens.

Another example is Operation MANGO, which shut down an American-owned beach-side resort for pedophiles located in Acapulco, Mexico. The resort was a haven for pedophiles that traveled to the facility for the sole purpose of engaging in sex with minors.

As a result of this investigation and others, the government of Mexico recently created a Federal task force to address crimes against children in their country.

The CyberSmuggling Center's technological capabilities include the National Child Victim Identification Program, a dynamic one-of-kind information system that will eventually contain all known and unique child pornographic images. The primary goal of the program is to help law enforcement agencies throughout the world locate and rescue children who have been victimized for sexual purposes.

This committee has asked that I address two specific concerns: one, the ease of access in transmission of child pornography on peer-to-peer file sharing networks; and two, the Bureau of Immigration and Customs Enforcement's efforts in tracking and investigating suspects that use this technology for criminal purposes. It was our privilege to assist the GAO in this study.

Considering the fact that there are now more than 20 peer-to-peer software applications available on the Internet, and that these applications are conducive to the unfettered transmission of images, both legitimate and illegal, the CyberSmuggling Center has taken the position that peer-to-peer networks do increase the likelihood of both intended and unintended exposure to child pornography.

The investigative effort of the CyberSmuggling Center, while extensive and highly successful, have been geared to attack the problem of child exploitation on a reactive basis. This posture is dictated primarily as a result of the enormous volume of child pornography-related tips received and processed by the CyberSmuggling Center.

The CyberSmuggling Center handles more than 1,500 tips per month. Each tip requires an initial review, resulting in a determination as to whether further investigation is warranted.

If referred for investigation, then evidence must be gathered and a perpetrator identified. This is a time consuming, labor-intensive process. The majority of the CyberSmuggling Center's resources are dedicated to tip response activities.

In contrast, the investigation of peer-to-peer networks can be classified as proactive in scope; that is, investigators with no prior information can actively enter publicly accessible file sharing networks, to detect illegal activity.

Recognizing the potential use of peer-to-peer file sharing by pedophiles, the CyberSmuggling Center re-assigned an intelligence analyst to begin examining these types of cases in February 2002. Today, the CyberSmuggling Center has referred more than 20 leads to the field, resulting in several successful enforcement actions, including the arrest of a known child abuser.

Although we have only scratched the surface, peer-to-peer file sharing networks have received and will continue to receive increased scrutiny by the CyberSmuggling Center. Searches can be tailored to reveal imagines of child pornography, prosecutorial venue can be claimed at either end of the transaction, evidence is easily captured and preserved on a real-time basis, and violators are readily identifiable by investigators with the requisite training and experience. For these reasons, peer-to-peer file sharing investigations are likely to increase.

In conclusion, let me reiterate that while we must, by necessity, continue to focus the majority of our attention and resources on the voluminous tips generated by outside entities, the CyberSmuggling Center will continue to expand its investigative efforts in the area of peer-to-peer file sharing.

I would like to thank the distinguished members of this committee for the opportunity to speak before you today, and I welcome the opportunity to answer any questions that you may have.

[The prepared statement of Mr. Netherland follows:]

STATEMENT OF J. MICHAEL NETHERLAND

CYBERSMUGGLING INVESTIGATIONS DIVISION

BUREAU OF IMMIGRATION AND CUSTOMS ENFORCEMENT

HOUSE COMMITTEE ON GOVERNMENT REFORM

MARCH 13, 2003

I. INTRODUCTION:

Mr. Chairman and distinguished members of the Committee, it is a privilege to appear before you today to discuss the CyberSmuggling Center 's efforts to combat child exploitation that is facilitated by the Internet. The CyberSmuggling Center, led by the Bureau of Immigration and Customs Enforcement, will continue its proud history of combating the sexual exploitation of children and the unfettered accessibility and illegal bartering of child pornography on the Internet via peer-to-peer file sharing networks. The peer-to peer file sharing network is but one more means by which pedophile predators ply their trade and victimize our children and the CyberSmuggling Center is expanding its investigative efforts to encompass this new technology.

II. OVERVIEW

The CyberSmuggling Center, located in Fairfax, Virginia, is recognized both nationally and internationally as a leader in the area of child exploitation investigations. The CyberSmuggling Center utilizes its resources and cutting edge technology as a means to protect our nation's children from sexual abuse and exploitation and has achieved great success in identifying and apprehending pedophiles. Recent investigative successes include:

- Operation HAMLET, a global investigation that resulted in the dismantlement of a ring of pedophiles who were molesting their own children and posting the images on the Internet for worldwide consumption. The CyberSmuggling Center, in its coordinative role, identified and rescued more than 100 children who were subjected to this torturous environment. The majority of these children were American citizens.
- Another example is Operation MANGO, which shut down an American-owned beachside resort for pedophiles located in Acapulco, Mexico. The resort was a haven for pedophiles that traveled to the facility for the sole purpose of engaging in sex with minors. As a result of this investigation and others, the government of Mexico recently created a federal task force to address crimes against children in its country.

The CyberSmuggling Center's technological capabilities include the National Child Victim Identification Program, a dynamic, one-of-a-kind information system that will eventually contain all known and unique child pornographic images. The primary goal of the program is to help law enforcement agencies throughout the world locate and rescue children who have been victimized for sexual purposes.

III. PEER-TO-PEER FILE SHARING NETWORKS

This Committee has asked that I address two specific concerns: (1) the ease of access and transmission of child pornography on peer-to-peer file sharing networks, and (2) the Bureau of Immigration and Customs Enforcement's efforts in tracking and investigating suspects that use this technology for criminal purposes.

A recent study undertaken jointly by the CyberSmuggling Center and the General Accounting Office (GAO) concluded that child pornography is easily accessed and transmitted via peer-to-peer file sharing networks. These networks are comprised of applications that allow subscribers to transfer various types of files, including image files, directly from one desktop to another in real time.

In its examination of peer-to-peer file sharing networks, the CyberSmuggling Center utilized twelve keyword search terms known by law enforcement to be associated with child pornography. Of the 1,286 files examined, forty-two percent (543) were determined to contain one or more images of child pornography. In another search utilizing just three keywords, nearly half of the files contained images classifiable as child pornography.

Keyword searches utilizing innocuous terms such as the names of cartoon characters and celebrities also produced multiple files containing child pornography. While the resulting percentages of illicit files were not nearly as high as for those generated using keywords typically associated with child pornography, the study concluded that the threat of inadvertent exposure to Internet users, including juveniles, is significant.

Considering the fact that there are now more than twenty peer-to-peer software applications available on the Internet and that these applications are conducive to the unfettered transmission of images both legitimate and illegal, the CyberSmuggling Center has taken the position that peer-to-peer networks increase the likelihood of both intended and unintended exposure to child pornography.

The investigative efforts of the CyberSmuggling Center, while extensive and highly successful, have been geared to attack the problem of child exploitation on a reactive basis. This posture is dictated primarily as a result of the enormous volume of child pornography-related "tips" received and processed by the CyberSmuggling Center.

The CyberSmuggling Center handles more than 1,500 "tips" per month. Each "tip" requires an initial review resulting in a determination as to whether further investigation is warranted. If referred for investigation, then evidence must be gathered and a perpetrator identified. This is a time consuming, labor-intensive process. The majority of the CyberSmuggling Center's resources are dedicated to "tip" response activities.

In contrast, the investigation of peer-to-peer networks can be classified as proactive in scope; i.e., investigators with no prior information can actively enter publicly accessible file sharing networks to detect illegal activity. Recognizing the potential use of peer-to-peer file sharing by pedophiles, the CyberSmuggling

Center reassigned an intelligence analyst to begin examining these types of cases in February 2002. To date, the CyberSmuggling Center has referred more than twenty leads to the field resulting in several successful enforcement actions including the arrest of a known child abuser.

Though we have only scratched the surface, peer-to-peer file sharing networks have received and will continue to receive increased scrutiny by the CyberSmuggling Center. Searches can be tailored to reveal images of child pornography, prosecutorial venue can be claimed at either end of the transaction, evidence is easily captured and preserved on a real-time basis, and violators are readily identifiable by investigators with the requisite training and experience. For these reasons, peer-to-peer file sharing investigations are likely to increase.

IV. CONCLUSION

In conclusion, let me reiterate that while we must, by necessity, continue to focus the majority of our attention and resources on the voluminous "tips" generated by outside entities, the CyberSmuggling Center will continue to expand its investigative efforts in the area of peer-to-peer file sharing.

I would like to thank the distinguished members of this committee for the opportunity to speak before you today and I welcome the opportunity to address any questions that you may have.

Chairman TOM DAVIS. Thank you very much.

Mr. Saaf, thank you for being with us.

Mr. SAAF. Thank you, Mr. Chairman, Congressman Waxman, and the rest of the committee. MediaDefender was founded in the summer of 2000, with the general business calling to fight Internet crime.

The biggest area of Internet crime in the summer of 2000 was obviously music piracy. That was because the peer-to-peer software program Napster only allowed the trading of music. You could not trade videos or images on that network. At the same time, there was a network that was created called the Gnutella Network, which was much smaller than Napster, but allowed the trading of all sorts of rich media files.

We observed a lot of pornography going across that network. It was pretty much the only peer-to-peer network where you could get pornography at the time. We also saw an alarming quantity of child pornography being shared on that network.

MediaDefender immediately called the FBI and the Department of Justice, and tried to alert the agencies to that fact. They received little attention.

Today, KaZaA is the 800 pound gorilla of peer-to-peer networking with, as you have mentioned, over 200 million downloads to date. Most of the video files and pictures on KaZaA are adult in nature.

There is the same child pornography problem that we observed in the summer of 2000, except it is 100,000 times larger now. There is 100,000 times the quantity of pornography and child pornography.

Porn spreads like music on a peer-to-peer network. The files are large. There is a high demand for it, and the copyright law is easily avoided on the networks.

MediaDefender took data from March 6th to March 10th of this month, to present some findings on child pornography on these networks. MediaDefender found 328,349 unique Internet addresses with files that appeared to be child pornography on them.

We also found 321,153 unique files that appeared to be child pornography by their name and file type. There are 4 million simultaneous users on the peer-to-peer networks at any one time approximately. The point is basically that there are a lot of users, and that all of them can get child pornography whenever they want.

Peer-to-peer users tend to feel a guiltless sense of anonymity. I want to say here that they should not feel anonymity at all in these networks. These are open, public networks, and it is easy for a company like MediaDefender to find these perpetrators and introduce them to law enforcement officials.

This is not like music, where law enforcement officials have been able to say, we cannot enforce the law against every single individual; there are too many. Child pornography is too dangerous for that.

Already, as we have heard, law enforcement officials around the Nation have started to actually prosecute cases on the peer-to-peer network. It is a relatively straight-forward procedure. A company like MediaDefender can gather the evidence and hand it over to a law enforcement official, where they conduct a normal child investigation Internet pornography case.

Just because it was easy and free to get the child pornography, that does not mean it gets to skirt the child pornography laws.

We also took some statistics on businesses, schools, and Government institutions that have potential child pornography on their networks, and I would like to go over those now.

This alarming trend of not caring about pornography on the networks can be seen in schools. We found over 800 universities in the Nation that had files on their networks that appear to be child pornography in nature.

I do not know how many schools there are in the United States, but I can assure you that most of the big schools are on that list.

I do not want to start naming names right now, but I will say that seven out of eight of the Ivy League schools had a combined total of over 190 computers that had files that appeared to be child pornography on their computers, sharing to the peer-to-peer network.

Hundreds of large companies are in this list, as well. It could be very embarrassing. I suggest that colleges and businesses start taking a proactive approach to get the child pornography off their networks, or block the peer-to-peer networks altogether.

The worst thing that MediaDefender found in its study was the government institutions that had child pornography on their networks; thousands of government computers with files that appear to be child pornography on them. It is ridiculous that Government resources could be used for something so unworthy as this.

The three most notable and largest on the list that we found were NASA, Los Alamos National Laboratory, and the Department of Defense.

What is very alarming about these is that they are secret or defense in nature; and what is really scary is, if pornography is accidently being shared on these networks, who knows what else is accidently being shared? Obviously, this is an information technology oversight.

There are no magic technology solutions for fixing the problem of pornography or child pornography on the peer-to-peer networks. Filtering only mildly helps the problem. This stuff changes so fast, everybody gets around the filters. It is just too easy.

There are 1 billion files in a constant state of flux on the peer-to-peer networks. You cannot identify what every file is.

Porn and child pornography will be an ever present problem on the peer-to-peer network, just like music piracy is. Thank you.

[The prepared statement of Mr. Saaf follows:]

Written Testimony for the Oversight Hearing on "The Prevalence of Pornography, Including Child Pornography, on Peer-to-Peer Networks"

By: Randy Saaf, President of MediaDefender, Inc.

March 13th, 2003

In the summer of 2000 Napster was hitting its stride as the hottest Internet software application since the web browser. As we all know, the primary use of Napster was for the illegal trading of copyrighted music over the Internet. This was the birth of the Peer-to-Peer ("P2P") movement that continues to build momentum even today. At its peak Napster had roughly 40,000,000 users, and it could only be used for downloading audio files (MP3s). Today, P2P networks (KaZaA, Gnutella, WinMX, etc.) have roughly 80,000,000 users and are used to trade all sorts of rich media including pictures, music, pornography, television shows, movies, and software.

MediaDefender was founded in the summer of 2000 with the company calling to "Fight Crime on the Internet." In the summer of 2000 there was one primary illegal activity occurring on the P2P networks and that was the trading of copyrighted material. However, MediaDefender quickly noticed the massive quantity of pornography being traded on the Gnutella network which was much smaller than Napster but allowed trading of all media types. Napster only allowed trading of music (MP3) files, so the savvy P2P users were going to Gnutella for their porn. P2P became very efficient for downloading porn for the same reasons it was very efficient for downloading MP3s: copyright law could be avoided and big files spread quickly across the network. Amongst the large quantity of normal porn, there was an alarming quantity of legally questionable porn. We were seeing file names fly across the network that were most likely child pornography. Not surprisingly, the same feelings of guiltless anonymity that made music stealing so predominant in the P2P world were also allowing child pornography to rapidly spread. MediaDefender tried to sell our policing technology to federal law enforcement agencies like the DOJ and the FBI, but received very little interest. So, MediaDefender had to build its business solely around P2P anti-piracy, which remains its core business to this day. Since then, MediaDefender has grown to be the primary provider of P2P anti-piracy technology in the world.

Napster eventually went away, and the KaZaA network filled the void for the hungry P2P users. There have been over 197,000,000 downloads of Kazaa to date. KaZaA allows the downloading of all types of media, including picture and video files. Naturally, the largest demand and supply for video files on Kazaa is adult content. Kazaa, and most of the other P2P networks, continue to have the same alarming child pornography problem MediaDefender observed in the summer of 2000, except now the quantity is about 100,000 times larger. MediaDefender took child porn data from the KaZaA network from 3/6/03 to 3/10/03. We basically used key words that a reasonable person would associate with child porn. That data is what is being referenced for all statistics in this report. MediaDefender found 328,349 unique IPs that were running KaZaA and sharing files that appeared to be child pornography. Presumably a unique IP is a unique computer or user excepting for dynamic IP addresses. MediaDefender found 321,153 unique movie and picture files on KaZaA that appear to be child pornography. There are roughly 4,000,000 users on KaZaA at any one time. We cannot determine the total number of people that used KaZaA over the course of our study, but it is obvious that there is a sizable child pornography presence on the network. It is also obvious that anyone can get child pornography on the network whenever they want it. I would suggest that there is probably no easier method in the word for acquiring child pornography than the P2P networks. I am concerned about the borderline pedophile that has not crossed that dangerous line yet, but it tempted to indulge his fantasy by the relative ease of the networks.

MediaDefender is primarily concerned with the child pornography problem on the P2P networks, although we realize the ease of availability of regular pornography raises an assortment of other societal issues. The fact that a 14 year old could use the same P2P network to download music and pornography is an obvious problem that I am sure will be adequately dealt with in this hearing. I want to raise the issue of that 14 year old accidentally downloading illegal child pornography to his parents' computer, and the district attorney in their county deciding to prosecute them because they are breaking a very well defined strict-liability child pornography possession law. That is a very scary scenario, but not as far fetched as it may seem. The same technology MediaDefender deploys to thwart piracy on the P2P networks can also be applied to find perpetrators of child pornography. Already, district attorneys around the nation have begun investigating cases of people sharing child pornography on P2P networks. These P2P users feel anonymous on the P2P networks, and many do not realize that the content they download is usually automatically shared up to the rest of the P2P network. Therefore, it is easy for MediaDefender to find these people. A district attorney or federal agent can give MediaDefender any school, business, or geographic region and we will probably be able to find an abundance of child pornography being shared on that IP block.

I want to make it clear that MediaDefender is never able to visually confirm the contents of the child pornography files because that, in itself, would be illegal, but the names of the files leave little doubt of their content. MediaDefender commonly finds multiple people at reputable companies and universities sharing 30 or more child pornography files apiece. MediaDefender's study found over 800 universities with computers on their networks sharing files that appeared to be child pornography. I do not know how many colleges there are in the nation, but I can assure you that almost every major college was in the list. I do not want to name names of schools and businesses at this point, but I do want to make the problem clear. Seven out of eight Ivy League schools had a combined total of over 190 computers that were serving content to the KaZaA network that appeared to be child pornography by its name and file type. Each computer probably represents a unique person at the university. It would be relatively simple for a law enforcement official to take that IP address and find the computer and student/employee it is associated with. It is also relatively simple for university officials to take that IP address and find the computer and student/employee it is associated with. I would suggest that universities and businesses start taking responsibility and proactively prevent child pornography from being served on their networks using P2P. MediaDefender also found hundreds of very large, reputable companies serving child pornography via P2P. With a couple guesses of some of the biggest companies in America, you would probably name some of the companies I am talking about. This could be very embarrassing for these companies if it ever comes out that company resources are being used to propagate the spread of child pornography. I would additionally suggest proactive prevention by businesses before there is a widespread law enforcement effort to stop this problem. Universities and businesses cannot trust their employees to "do the right thing." Most of these students/employees are unaware that they are re-sharing the illegal child pornography they downloaded to the rest of the P2P network and that they can be easily seen by a company like MediaDefender. So, the combination of their perverseness and ignorance creates slam-dunk evidence for a policing organization to get a search warrant to walk in and seize the perpetrators hard-drive which contains the child porn. Colleges and businesses have the means to monitor the traffic on their networks and should be more responsible for illegal activity that is taking place on it.

It is unacceptable that so many of our countries most reputable universities and businesses are unwittingly dedicating their resources to the spread of child pornography. However, even more alarming is the quantity of pornography and child pornography MediaDefender finds at government institutions. Thousands of government computers are sharing pornography, including child pornography, files at many of our countries most important institutions. Heads should roll for this one because it is absolutely ridiculous that government resources are being poached for this cause. I also want to make it clear that these are not isolated slip-ups in IT. Generally, if a government organization has one computer sharing pornography on P2P, it will have at least twenty others. Of course, this also raises the very important issue of security. Many of these organizations MediaDefender found are "top secret" or defense in nature. If the people running these institutions' information technology are too inept to not realize their networks are being used to share pornography on P2P, who know what other content might be accidentally shared via P2P? One careless individual working on a top secret project accidentally sharing his entire C-drive could cause extreme havoc. If MediaDefender can monitor these government institutions for holes in their IT facilitated by P2P, so can our countries enemies. Information technology at these government organizations is clearly lacking and may be creating severe security risks for our country. Government institutions should have the knowledge and resources to prevent IT problems associated with P2P, and they should be forced to do so immediately.

There are no magic technology bullets for solving the problems associated with P2P networking. Technologies such as filters will only mildly quash the problem of P2P child pornography. The community of people sharing child pornography on the P2P networks has already devised naming codes to attempt to hide the actual content. Typically, these naming codes will be an elaborate assortment of letters and symbols that are commonly understood in the child pornography P2P community. For example, "R@ygold" is a common naming code right now. Further, there are almost a billion files on P2P at any one time. You just cannot look at what every files' content contains, and even if you could, there is a constant state of flux around what files are shared. As soon as you identify one set of a billion files, another set of a billion files will sprout up. That is the nature of the networks. Unless a P2P network is centrally run and only allowed to distribute a closed set of content, there will never be a practical technology for preventing "illegal" content while allowing "legal" content.

The reality is that child pornography will be an ever present problem on P2P networks the same way that music piracy is an ever present problem on P2P networks. Child pornography is the highest form of unprotected speech, and law enforcement officials in both local and federal government have a duty to enforce the existing child pornography laws. P2P may seem and feel ethereal, but there are actual people at the end of every peer. Law enforcement officials must deploy technology, like MediaDefender's, to find and prosecute perpetrators of child pornography on the P2P networks.

Chairman TOM DAVIS. Thank you very much.

Mr. Rung.

Mr. RUNG. Good morning, Mr. Chairman and members of the committee, my name is Daniel Rung. I am the founder of Grokster, one of the more popular file sharing programs on the Internet today.

I would like to thank you for inviting me to testify today on file sharing and pornography, and in particular, child pornography.

The Internet is a communications tool that allows for the easy storage and virtually instantaneous transfer of all types of information, including pornographic material. The Internet pornographic industry is generally considered to be one of the most successful and widespread on the Internet. One could argue that pornography is ubiquitous on the Internet.

One of the side effects of this ready availability of pornographic material is children's easy access to it, either intentionally or accidently.

Before the development of peer-to-peer file sharing programs, pornography could be easily found on free and pay Web sites, news groups, FTP sites, and so on. Many fairly effective tools were then developed to allow users to filter out certain types of Internet content, including pornography. Then peer-to-peer file sharing programs were developed and launched on the Internet.

Although these file sharing programs were not designed with pornography in mind, today's file sharing programs provide a new avenue of access to this type of material. Since today file sharing programs have no control over the contents that users share with other users, it is easy for a child user to encounter such pornographic material.

It has been estimated that as much as 50 percent of the files created through file sharing programs consist of pornographic material; and unfortunately, just like the rest of the Internet, some unknown amount of that is child pornography.

In an attempt to allow users to filter out objectional material, many file sharing programs now have what we call bad word filters. These filters can be set to screen out much objectional material from the search results.

Additionally, the providers of third party content filtering programs such as Net Nanny and Cybersitter have been successfully developing techniques to allow users to filter or block objectional material from file sharing programs.

What, specifically, can parents do to keep this material from their children? First, educate your children, as appropriate for their age, to be aware that this type of material exists and what to do if they should encounter it.

Second, supervise your children while they are using the Internet. Observe what Web sites they visit and what programs they are using.

Third, consider restricting your children's level of user access on the computer. Using settings in the Windows operating system, parents can create a special account for each child called a restricted user account.

This restricted user account has default settings that will block the child from installing any software on the computer, including peer-to-peer file sharing programs. I understand these restricted user accounts may also be customized to allow varying amounts of access to all the functions in the Windows operating system.

Fourth, install and properly configure one of the numerous content filtering programs. Some can be said to filter or even block access to file sharing programs. Periodically, review the programs installed on the computer to ensure that they meet with your approval.

Last, when installing any file sharing software, go through all of its settings, to ensure that they are set to block any objectionable material. Set up the password protection if it is available in that program. To summarize, educate, supervise, restrict, filter, and configure.

As a parent and grandparent, I share this committee's concern with child pornographers and their customers. We at Grokster maintain a very clear and open policy in relation to child porn. We do not want child pornography on Grokster.

We encourage users to report this type of material to the appropriate authorities. We have previously cooperated with law enforcement officers, and would gladly do so again to combat child pornography.

Sadly, child pornography continues to be available through the Internet. There are already many existing laws that deal with child pornography. Using these laws, child pornographers and their customers can be brought to justice to stop their abuse of defenseless children.

The law enforcement resources brought to bear on this problem to date seem to be too little. I urge the members of this committee to bring more law enforcement resources to bear on this continuing problem.

Thank you for holding this important hearing, and I look forward to working with the committee on these issues in the future.

[The prepared statement of Mr. Rung follows:]

STATEMENT of

Daniel Rung
Founder
Grokster, Ltd.

On File Sharing and Pornography

Before the

Committee on Government Reform
United States House of Representatives

FILE SHARING AND PORNOGRAPHY

March 13, 2003

Good morning, Mr. Chairman and members of the Committee, My name is Daniel Rung. I am the founder of Grokster, one of the more popular file sharing programs on the Internet today. I would like to thank you for inviting me to testify today on file sharing and pornography and, in particular, child pornography.

The Internet is a communications tool that allows for the easy storage and virtually instantaneous transfer of all types of information, including pornographic material. The Internet pornographic industry is generally considered to be one of most successful and widespread on the Internet. One could argue that pornography is ubiquitous on the Internet. One of the side effects of this ready availability of pornographic material is children's easy access to it, either intentionally or accidentally.

Before the development of peer to peer file sharing programs, pornography could be easily found on free and pay websites, usenet news groups, ftp sites, and so on. Many fairly effective tools were then developed to allow users to filter out certain types of Internet content including pornography. Then peer to peer file sharing programs were developed and launched on the Internet.

Although these file sharing programs were not designed with pornography in mind, today's file sharing programs provide a new avenue of access to this type of material. Since today's file sharing programs have no control over the contents that users share with other users, it is easy for a child user to encounter such pornographic material.

It has been estimated that as much as fifty percent of the files traded through file sharing programs consist of pornographic material. And unfortunately, just like the rest of the Internet, some unknown amount of that material is child pornography.

In an attempt to allow users to filter out objectionable material, many file sharing programs now have "bad word" filters. These filters can be set to screen out much objectionable material from the search results. Additionally, the providers of third party content filtering programs, such as Net Nanny and CyberSitter, have been successfully developing techniques to allow users to filter or block objectionable material from file sharing programs.

So, what specifically can parents do to keep this material from their children?

First, educate your children, as appropriate for their age, to be aware that this type of material exists and what to do if they should encounter it.

Second, supervise your children while they are using the Internet. Observe what websites they visit and what programs they are using.

Third, consider restricting your children's level of user access on the computer. Using settings in the Windows operating system, parent's can create a special account for each child called a "restricted user" account. This "restricted user" account has default settings that will block the child from installing any software on the computer, including peer to peer file sharing programs. I understand these "restricted user" accounts may also be customized to allow varying amounts of access to all the functions in the Windows operating system.

Fourth, install and properly configure one of the numerous content filtering programs. Some can be set to filter or even block access to file sharing programs. Periodically, review the programs installed on the computer to ensure they meet your approval.

Last, when installing any file sharing software, go through all of its settings to ensure that they are set to block any objectionable material. Set up the password protection if it is available on that program.

To summarize: Educate. Supervise. Restrict. Filter. Configure.

As a parent and grandparent, I share this committee's concern with child pornographers and their customers. We at Grokster maintain a very clear and open policy in relation to child porn, "We do not want child pornography on Grokster." We encourage users to report this type of material to the appropriate authorities. We have previously cooperated with law enforcement officers and will gladly do so again to combat child pornography.

Sadly, child pornography continues to be available throughout the Internet. There are already many existing laws that deal with child pornography. Using these laws, child pornographers and their customers can be brought to justice to stop their abuse of defenseless children. The law enforcement resources brought to bear on this problem seem to be too little. I urge the members of this committee to bring more law enforcement resources to bear on this continuing problem.

Thank you for holding this important hearing, and I look forward to working with the committee on these issues.

Chairman TOM DAVIS. Mr. Rung, thank you, and thank you for being with us today.

Mr. RUNG. Thank you.

Chairman TOM DAVIS. Dr. Greenfield.

Ms. GREENFIELD. Mr. Chairman, Congressman Waxman, distinguished members of the committee, thank you very much for inviting me to speak to you today.

My name is Dr. Patricia Greenfield. I am a developmental psychologist and professor in the Department of Psychology at UCLA. I currently direct the UCLA Children's Digital Media Center, under a grant from the National Science Foundation.

I am a member of the National Academy of Science's Board on Children, Youth, and Families; and I participated in their workshop on non-technical strategies to reduce children's exposure to inappropriate material on the Internet.

It is an honor to talk with you today about pornography on peer-to-peer file sharing networks, as it relates to child development and families. But before I speak on that subject, I want to add one technical word to the presentation so far.

In our lab, in preparation for this, we did some tests of the internal filters that KaZaA provides. No. 1, they are password protected, so presumably a parent could keep a child from interfering, once they set them; and second, we found two of the three filters proved very successful. One filter, for example, allows you to filter out all images, and I think that works very, very well.

So I want you to keep that in mind, because you could perhaps require these types of filter systems or strongly suggest them to be in all of these file sharing programs.

Now I want to move to my prepared remarks that relate to child development, families, and pornography. I want to focus on three questions, and I will begin with these questions and a summary of my answers. Fuller answers can be found in my written testimony, as well as references to the relevant research that I am drawing on.

First question, what effect does pornography in peer-to-peer file sharing programs have on children's development? Let me give an example of such effects.

One study found that 13-year-olds and 14-year olds became more accepting of pre-marital and extra-marital sex, after seeing sexual relations between unmarried, but not married, partners on video. This example shows one route by which pornography can affect the moral values of young teenagers.

Equally important, use of pornography can be an important additional risk factor for sexual violence, when used heavily by boys already at risk for anti-social behavior.

A study of long-term memories of impactful experiences with sexual media in college students indicates that inadvertent or unintentional exposure can be both frightening and disgusting to children and teens, especially girls.

In sum, the evidence indicates that pornography and other sexualized media can influence sexual violence, sexual attitudes, moral values, and sexual activity of children and youth.

Second question, what are the challenges parents face in reducing their children's access to pornography on peer-to-peer networks and elsewhere? We have already heard a lot about this.

One important challenge that has been mentioned is the fact that these programs, originally developed for music, have recently become the most popular use of the Internet for pre-teens and teens; occupying an average of 32 minutes a day, and that is an unselected, kind of middle class sample.

These are the same peer-to-peer networks that can, of course, as we have heard, contain pornography and other materials. Such networks, however, are part of an all-pervasive sexualized media environment.

This total environment leads to a tremendous amount of inadvertent and unintentional exposure of children and young people to pornography and other adults sexual media.

For example, on peer-to-peer file sharing programs, banner ads provide a source of inadvertent exposure to what, for children and teens, could be precocious sexuality.

You saw some screens up there, and they had kind of an innocuous banner as in the lower left hand corner, for example, for Nokia phones. But when I did my test, I found adds floating through for female condoms, male condoms, and introduction to potential sexual partners through personal ads.

These banner adds, as you saw today, are viewed as soon as one enters the program. They cannot be controlled by the user. This inadvertent and unintentional exposure to sexualized media is a major challenge to parents.

Third question; what are the non-technical means that parents can use to deal with these challenges? We have already heard some ideas from Mr. Rung.

Let me add, a warm and communicative parent/child relationship is the most important weapon that parents have. Such a relationship, research has shown, reduces the sexual risktaking that can be stimulated by pornography.

An open family communications style is another powerful weapon. For example, one study indicated that such a style mitigated the effects of video portrayals of non-marital sex on the moral judgments of 13 and 14 year-olds.

Therefore, in today's media environment, an open communication style within the family is critical. In addition, open parent/child channels for communicating specifically about sexual and media experiences, that is very useful; second, sex education at home or school; and third, parental participation with children on the Internet; all of these are constructive influences that can mitigate negative effects of pornography.

Finally, for boys already at risk for anti-social behavior, parent should carefully monitor and severely limit access to pornography on file sharing networks and elsewhere.

Let me close by talking a little bit about some important issues in need of future research. Pornography on peer-to-peer file sharing networks is not unique, but it is part of a highly sexualized media environment. By analogy to television and violence research, one likely developmental outcome of over-exposure to sexual media is desensitization. Another outcome is the culture of the body, especially for females.

But how does desensitization affect the emerging sexuality of young people? What are the psychological costs and benefits of this body culture? What is the role of other media in these processes? All these are areas where we need further research, and there are many other questions.

What type of experiences are children and young people having with sexual material on peer-to-peer file sharing networks? What are the long-term effects of these experiences? How do parents view the challenges of the sexually saturated media environment for child rearing and child development?

What are the effects on children and families of different parental strategies vis-a-vis sexual and pornographic material on the Internet? These are important questions greatly in need of more research and more research funding; thank you very much.

[The prepared statement of Dr. Greenfield follows:]

Testimony to the Committee on Government Reform, Congress of the United States, House of Representatives, March 13, 2003

Patricia Marks Greenfield, Professor of Psychology, UCLA

My name is Dr. Patricia Greenfield. I am a developmental psychologist and Professor in the Department of Psychology at UCLA. I currently direct the UCLA Children's Digital Media Center, under a grant from the National Science Foundation. I am a member of the National Academy of Sciences' Board on Children, Youth, and Families, and I participated in their Workshop on Nontechnical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet. It is an honor to talk with you today about pornography on peer-to-peer file sharing networks, as they relate to child development and families.

Overview

My remarks this morning will focus on three questions. I begin with these questions and with a summary of my answers:

1. What does pornography on peer-to-peer filesharing programs (and elsewhere) mean to children and their development?

In sum, the evidence indicates that pornography and related sexual media can influence sexual violence, sexual attitudes, moral values, and sexual activity of children and youth.

2. What are the challenges parents face in reducing their children's access to pornography on peer-to-peer networks and elsewhere?

In sum, peer-to-peer file sharing networks are extremely popular with young people. They are part of an all-pervasive sexualized media environment. This total environment, including filesharing networks, leads to a tremendous amount of inadvertent and unintentional exposure of children and young people to pornography and other adult sexual media. Peer-to-peer networks and the Internet differ from other sexualized media in that young people construct important components of this sexualized environment themselves.

3. What are the nontechnical means parents can use to deal with these challenges?

A warm and communicative parent-child relationship is the most important factor. In addition, open parent-child channels for communicating about sexual and media experiences, sex education at home or school, and parental participation with children on the Internet are constructive influences. Finally, for boys already at risk for antisocial behavior, parents should carefully monitor and severely limit access to pornography on filesharing networks and elsewhere.

File Sharing, Pornography, Child Development, and Family Issues in Detail

Question 1. What does pornography on peer-to-peer file sharing networks (and elsewhere) mean for children and their development?

A. Consumption of sexual media is related to the sexual activity and attitudes of adolescents. (This applies not just to pornography but to other types of files that are circulated on peer-to-peer file sharing networks.)

i. A number of surveys, from junior high to college, indicate that exposure to MTV (very common files on peer-to-peer networks) and R-rated films are correlated with premarital sexual permissiveness (Malamuth & Impett, 2001). Experimental studies confirm that exposure to music videos such as those seen on MTV can actually liberalize attitudes toward premarital sex, and this is particularly true for girls (Malamuth & Impett, 2001).

ii. In a field experiment, college students viewed R-rated films suggesting positive effects of sexual aggression (e.g., the sexual arousal of the victim). Viewing this type of film made male students significantly more accepting of the use of aggression against women in sexual and nonsexual interactions (Malamuth & Check, 1981). This finding concerning R-rated films is relevant to file sharing networks because violent pornography, found on these networks, also shares these characteristics.

iii. Video portrayals of sexual relations between unmarried partners – an all-pervasive characteristic of pornography – affected 13- and 14-year-olds' moral judgments concerning premarital and extramarital sex: their judgments became more accepting after viewing video portrayals of sexual relations between unmarried partners. In contrast, video portrayals of sex between married individuals had no effect on moral judgments (Bryant & Rockwell, 1994). There was, however, no "spillover" effect of viewing sexual relations between unmarried partners into nonsexual areas of moral judgment, such as judgments concerning criminal or antisocial behavior.

B. Pornography has an adverse effect on older adolescent boys and young men already at high-risk for aggressive behavior.

High risk factors include impulsivity, hostility to women, and promiscuity. In this group, very frequent use of pornography is associated with a much higher rate of sexual aggression than found in youth of the same risk level who use pornography somewhat, seldom, or never (Malamuth, Addison, & Koss, 2000).

C. Memories of impactful sexual media from childhood and adolescence are overwhelmingly negative.

College students were asked to recall one impactful sexual media experience from their earlier lives and their responses to it; the most common emotional responses to the sexual film or video they recalled were disgust (24.5%), shock or surprise (23.6%), and embarrassment (21.4%)

(Cantor, Mares, & Hyde, 2001). Other negative emotional responses were anger (18.4%), fear (11.2%), sadness (9.2%). Only two positive emotions were mentioned (interest and happiness or pleasure) and these were mentioned by only a small minority of respondents.

In terms of physical (as opposed to emotional) reactions, sexual arousal was mentioned by fewer than 17% of the participants. There seems to be no reason not to extrapolate a low rate of sexual response to pornography on peer-to-peer networks, especially when the exposure is inadvertent (very frequent, as we shall see in the next section).

Responses differed according to the age at which the recalled sexual medium had been experienced. When experienced at age 12 or younger, embarrassment, fear of being caught, guilt, and confusion were significantly more common than when experienced at age 13 or older. Learning about biology and sex behaviors were also significantly more common in the earlier rather than later memories. On the other hand, the reactions of nausea, crying, disgust, anger, and sadness were more common for recalled media experiences that had taken place at age 13 or older. Where there were significant gender differences, positive or neutral memories were more common for males than for females (nudity, arousal, interest), whereas negative or neutral memories were significantly more common for females (dialog, rape, crying, and sadness). We must conclude that sexual media, including pornography, have different meanings and impacts on girls and boys.

Although in the minority, effects were sometimes enduring. Here the effects were most frequently neutral, followed by negative effects such as confusion (9.7%) and unwanted recurring thoughts (7.7%). Reduced eagerness to have sex was mentioned by 6.1% of respondents. This could be considered to be either positive or negative, depending on one's moral perspective and the age or situation (e.g., married, unmarried) of the respondent. A small minority (4.1%) mentioned learning about biology, sexual risks, or sex behaviors from the impactful sexual medium they remembered. For a slightly larger percentage (5.1%), the recalled impactful media experience reinforced moral beliefs or made them aware of sex without love. (A given media experience could have more than one subjective impact.)

In sum, exposure to impactful sexual media up through the college years was overwhelmingly negative with a fairly low rate of recalled sexual response. Effects differed by gender, with girls experiencing more negative effects and boys experiencing more positive effects. Effects were sometimes longlasting. Extrapolating from these findings, we can infer that the memories of impactful sexual media of current college students would, on the one hand include the Internet, including peer-to-peer filesharing, and, on the other hand, be overwhelmingly negative, especially for girls, with some enduring effects and a relatively low rate of sexual response.

2. What are the challenges parents face in reducing their children's access to pornography on peer-to-peer networks and elsewhere?

A. Filesharing programs, originally developed for music, were, as of the end of 1999 and the beginning of 2000, the most popular use of the Internet for preteens (seventh graders) and teens (tenth graders) (Gross, Juvonen, & Gable, in preparation).

In a somewhat ethnically diverse sample of middle- to upper-middle SES population, 91% of participants reported at least some Internet use at home. In the total sample, participants reported downloading music an average of 32 minutes a day. These are the same peer-to-peer networks that contain pornography and other materials.

B. The presence of pornography on filesharing programs is continuous with what is available and consumed on other media.

Availability. As early as 1992, the most popular prime time shows with children and adolescents stressed physical appearance for women and scoring for men (Ward, 1995). The former value at very least has now permeated our culture (L. Greenfield, 1993). Similarly, in pornography, most of the emphasis is on physical attributes, with no depiction of emotional or relational elements (Malamuth & Impett, 2001). "Most commonly the portrayals are of female nudity and of men having sex with numerous, easily accessible young women" (Malamuth, 2001).

Consumption. This type of visual material is consumed primarily by males. In contrast, romance novels, a purely verbal form of sexual media, are consumed primarily by females.

Perhaps most pertinent to the issue of pornographic filesharing in peer-to-peer networks on the Internet is the rate of consumption of other pornographic media by children and youth. In a study of R- and X-rated media in the early 1980s, Bryant (1985) found that, by age 15, 92% of males and 84% of females had looked at or read *Playboy* or *Playgirl.* By 18, the proportion had risen to 100% for males and 97% for females. The average age of first exposure was reported to be 11 for males and 13 for females. Similarly, 92% of thirteen to fifteen year-olds had said that they had already seen an X-rated film; the average reported age of first exposure was 14 years 8 months.

It is possible however that the Internet (apart from peer-to-peer file sharing) is lowering the age of first exposure to such material. In a survey published in 1998, 48% of third- through eighth graders reported having visited Internet sites with various types of "adult" content. Sexual sites were the most popular of the adult Internet sites (Kahn-Egan, 1998).

C. Inadvertent or unintentional exposure of children and teens is an issue in file sharing networks and other sexual media.

We know from the Govenment Reform report presented this morning that inadvertent exposure to pornography on peer-to-peer filesharing networks is a problem. However, it is a problem that is not restricted to peer-to-peer networks or even to the Internet. Indeed, inadvertent or unintentional exposure to sexual material is a general challenge for parents in today's media environment.

When over 200 college students were asked to recall an instance of sexual media content that had a strong effect on them, almost 85% reported on a movie whose rating (R, X, or NC-17) suggested that they were, at the time, too young to see it. Considering the total sample of recalled media content, only a small minority (29.1%) had actively sought to view it themselves. "The most common scenario was that the respondent watched the program or movie because someone else wanted to watch it (40.8%), but almost a third (30.1%) said they just happened to stumble upon the material" (Cantor, Mares, & Hyde, 2001, p. 19). When the impactful sexual medium experience occurred at age 12 or less, it was usually because someone else was watching it. When it occurred at age 13 or older, the respondent usually either sought it out or inadvertently stumbled into it.

As in peer-to-peer filesharing networks, peers were crucial intermediaries, albeit known rather than unknown peers. That is, most respondents reported viewing with someone else, most commonly a friend.

D. On peer-to-peer filesharing programs, banner ads provide a source of inadvertent exposure to sexuality.

For example, banner ads promote the sale of female condoms, male condoms (Figure 1), and introductions to potential sexual partners through personal ads (Figure 2). These are viewed as soon as you enter the program. They cannot be controlled by the user.

E. In peer-to-peer networks, pornographic files are not just passively consumed, advertently or inadvertently, by young people. Young people actively seek them out and make them available to others.

An important characteristic of these networks is that they are created by the users. Therefore, if a high proportion of users are teenagers, it is also the case that a high proportion of the distributors are also teenagers. That is, music videos and X-rated files have been downloaded and made available to others by the same young people who are consuming them. This is similar to teen chat rooms, where a high proportion of the talk is about sex, and this sexualized talk is created by the chatters themselves (Greenfield, 2000; Greenfield & Subrahmanyam, submitted for publication; Ianotta, ,2001).

Question 3. What are the nontechnical means parents can use to deal with these challenges?

A. Maintain an open family communication style.

With 13- and 14-year-olds, effects on moral judgments of sexual portrayals of non-marital sex on video (characteristic of pornography on peer-to-peer file sharing networks) were mitigated by an open family communication style (Bryant & Rockwell, 1994). Therefore, in today's media environment, an open communication style within the family is critical

B. Be open to discussing sex with your children.

People raised in families where sex is treated as taboo may be more susceptible to the influences of sexually explicit media than those reared in homes where sex is a permissible subject of conversation (Malamuth & Billings, 1985; Gunter, 2002). However,

C. Communicating about specific sexual topics is less important than developing and maintaining a warm and communicative parent-child relationship.

A warm and communicative parent-child relationship reduces sexual risk-taking (Miller, Benson, & Galbraith, 2001).

D. Make sure that your child gets sex education.

People raised with little education about sexuality seem to be more vulnerable to influences of sexually explicit media than people raised with more education about sexuality (Gunter, 2002; bMalamuth & Billings, 1986).

E. Discuss media experiences witth your child.

In a study of thousands of high school students, girls who less frequently discussed media experiences with their parents had nearly twice the exual experience rate of those whose discussions were more frequent (Peterson, Moore, & Furstenberg, 1991).

F. Use the Internet (and other media) with your child.

Girls who watched television apart from their parents had more than three times the rate of sexual experiences as those who watched with their parents. Boys who watched television apart from their parents showed a significant correlation between viewing time and sexual experience; boys who watched with their parents did not. That is, co-viewing removed any impact of viewing time on sexual experience. This advice is based on a correlational study (Peterson, Moore, & Furstenberg, 1991), which cannot by itself prove a causal relationship between co-viewing and child effects. However, experimental research on nonsexual television (which can prove causal relations) indicates that co-viewing with parents, who discuss the media content with the child, can indeed remove or mitigate negative impacts of antisocial television (Singer & Singer, 1986).

Using the Internet with one's child is facilitated by rules that limit Internet use when parents are not around, such as requiring the child to ask permission to use the Internet and limiting the number of hours the child can use the Internet. Such measures are already taken by more than 60% of parents with Internet access at home, more so with younger than older adolescents (UCLA Center for Communication Policy; Gross & Gable, 2002). These facts suggest something else that parents can do:

G. Put the computer in a public place in your home; if at all possible, do not let your child have a computer with internet access in his or her room.

This will help accomplish what about 90% of parents with Internet access report doing, keeping an eye on what children do with the Internet (Center for Communication Policy).

H. If you have a child with antisocial tendencies, restrict use of the Internet, including file sharing, to supervised sessions.

Restrict other access to pornography to the maximum possible. Frequent use of pornography by high risk males is associated with and seems to produce a large increase in sexual aggression (Malamuth, 1993). In general, strict rules are more effective than flexible ones (Gross, Juvonen, & Gable, in preparation). Nanny or filtering software, already used by about 32% of families with Internet access (UCLA Center for Communication Policy), can help in this effort, but filters are not perfect, as the Government Reform Committee report, also presented today, indicates.

Important Issues in Need of Future Research

Pornography on peer-to-peer file sharing networks is not unique, but is part of a highly sexualized media environment. By analogy to television and violence research, one likely developmental outcome of overexposure to sexual media is desensitization. Another outcome is the culture of the body, especially for females (L. Greenfield, 2002). But how does desensitization affect the emerging sexuality of young people? What are the psychological costs and benefits of this body culture? What is the role of other media in these processes?

Many other questions remain. What type of experiences are children and young people having with sexual material on peer-to-peer file sharing networks? What are the longterm effects of these experiences? How do parents view the challenges of the sexually-saturated media environment for child rearing and child development? What are the effects on children and families of various parental strategies vis-à-vis sexual and pornographic material on peer-to-peer networks and the Internet more generally? These are important questions greatly in need of more research and more research funding.

Summary

1. What does pornography on filesharing programs (and elsewhere) mean to children and their development?

In sum, the evidence indicates that pornography and related sexual media can influence sexual violence, sexual attitudes, moral values, and sexual activity of children and youth.

2. What are the challenges parents face in reducing their children's access to pornography on peer-to-peer networks and elsewhere?

In sum, peer-to-peer file sharing networks are extremely popular with young people. They are part of an all-pervasive sexualized media environment. This total environment, including file sharing networks, leads to a tremendous amount of inadvertent and unintentional exposure of children and young people to pornography and other adult sexual media. Peer-to-peer networks and the Internet differ from other sexualized media in that young people construct important components of this sexualized environment themselves.

3. What are the nontechnical means parents can use to deal with these challenges? A warm and communicative parent-child relationship is the most important factor. In addition, open parent-child channels for communicating about sexual and media experiences, sex education at home or school, and parental participation with children on the Internet are constructive influences. Finally, for boys already at risk for antisocial behavior, parents should carefully monitor and severely limit access to pornography on filesharing networks and elsewhere.

Acknowledgments

I would like to express my appreciation to: Dr. L. Monique Ward, Developmental Psycyhology, University of Michigan; Dr. Neil Malamuth, Communication Studies, UCLA; Drs. Jeffrey Cole and Michael Suman, UCLA Center for Communjication Policy, and Elisheva Gross and Janet Tomiyama, UCLA Children's Digital Media Center. This testimony could not have been prepared without their crucial input and help.

References

Bryant, J. (1985). Frequency of exposure, age of initial exposure, and reactions to initial exposure to pornography [Report presented to the Attorney General's Commission on Pornography, Houston, TX]. In D. Zillman & J. Bryant (Eds.), *Pornography: Research Advances and Policy Considerations.* Hillsdale, NJ: Erlbaum.

Bryant, J. & Rockwell, S. C. (1994). Effects of massive exposure to sexually oriented prime-time television on adolescents' moral judgment. In D. Zillmann, J. Bryant, & A. C. Huston (Eds.), *Media, children, and the family.* Hillsdale, NJ: Lawrence Erlbaum.

Cantor, J., Mares, m-l, & Hyde j. s. (2001). Autobiographical memories of exposure to sexual media content. Paper presented at the Biennial Meeting of the Society for Research in Child Development, Minneapolis, MN.

Greenfield, L. (2002). *Girl culture.* San Francisco: Chronicle Press.

Greenfield, P. Developmental issues (2000, December) Paper prepared for the Workshop on Nontechnical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet. National Academy of Sciences, Washington, DC.

Greenfield, P. M. & Subrahmanyam, K. (submitted for publication). Online discourse in a teen chatroom: New codes and new modes of coherence in a visual medium.

Gross, E. F. & Gable, S. E. (2002). The impact of online communication on the social adjustment and well-being of early and mid adolescents. Presented at the Society for Research on Adolescence, New Orleans.

Gross, E. F., Juvonen, J., & Gable, S. E. (in preparation). A comparison of early and mid-adolescents' Internet use and social adjustment.

Gunter, B. (2002). *Media sex: What are the issues?* Mahwah, NJ: Erlbaum.

Ianotta, J. G. (2001). *Nontechnical strategies to reduce children's exposure to inappropriate material on the Internet: Summary of a workshop.* Washington, DC: National Academy Press.

Kahn-Egan, C. N. (1998). *Pandora's boxes: Children's reactions to and understanding of television rules, ratings, and regulations.* Unpublished doctoral dissertation, Florida State University.

Malamuth, N M (1993). Pornography's impact on male adolescents. *Adolescent Medicine: State of the Art Reviews, 4,* 563-575.

Malamuth, N. M., Addison, T., & Koss, M. (2000). Pornography and sexual aggression: Are there reiliable effects and can we understand them? *Annual Review of Sex Research, 11,* 26-91.

Malamuth, N. M. & Billings, V. (1986). The functions and effects of pornography: Sexual communication vs. the feminist models in the light of research findings. In J. Bryant and D. Zillman (Eds.), *Perspectives on media effects.* (pp. 83-108). Hillsdale, NJ: Erlbaum.

Malamuth, N. M. & Check (1981). The effects of mass-media exposure on acceptance of violence against women: A field experiment. *Journal of Research in Personality, 15,* 436-446.

Malamuth, N. M. & Impett, E. A. (2001). Research on sex and the media: What do we know about effects on children and adolescents? In D. G. Singer & J. L. Singer (Eds.) (2001). *Handbook of Children and the Media* (pp. 269-287). Thousand Oaks: Sage.

Singer, J. L. & Singer, D. G. (1986). Family experiences and television viewing as predictors of children's imagination, restlessness, and aggression. *Journal of Social Issu;es, 42,* 107-124.

UCLA Center for Communication Policy. The UCLA Internet Report – Surveying the digital future.

Ward, L. M. (1995). Talking about sex: Common themes about sexuality in the prime-time television programs children and adolescents watch most. *Journal of Youth and Adolescence, 24,* 595-615.

Chairman TOM DAVIS. Dr. Greenfield, thank you very much. I am going to just ask one question, and then yield to Mr. Waxman and let other Members have a chance.

Mr. Rung, thanks a lot for being here today. I think you can add a lot to this, just from your experience. But what is Grokster's business model? How do you end up making money in this?

Mr. RUNG. Basically, it is through advertising revenues. As a matter of fact, I was making a note, when Dr. Greenfield was speaking, about the fact that we do, in fact, have these banner ads flashing across the face of it, whether you like it or not as a user. I do intend to go back and review the subject matter.

Chairman TOM DAVIS. So advertising is basically how you make your money?

Mr. RUNG. Yes, basically advertising, yes.

Chairman TOM DAVIS. And you do not have any control over the content. People can then put anything in they want and trade back and forth.

Mr. RUNG. That is correct.

Chairman TOM DAVIS. It is like a telephone company, almost.

Mr. RUNG. That would be a good analogy.

Chairman TOM DAVIS. That is my first question.

Mr. Waxman.

Mr. WAXMAN. Thank you, Mr. Chairman; well, to followup on that, Mr. Rung, when people go on to Grokster or some of these other file sharing sites, and they want to download something about Britney Spears or the Olsen twins or Pokemon, why is it that they get this pornography?

Mr. RUNG. Because you are searching for basically a word; in other words, they are putting in, say, Britney Spears, and it searches not just the title, but also there are some tags attached to the files. The users can set those tags in a particular file, plus, they can mis-name files.

Mr. WAXMAN. Well, is anybody making money out of this?

Mr. RUNG. Between the users themselves, not that I am aware of, unless the pornography industry perhaps is.

Mr. WAXMAN. Well, is the pornography industry making any money?

Mr. RUNG. Well, overall, I believe yes, from what I read on the Internet; but as specifically related to file sharing, I really am not sure.

Mr. WAXMAN. Well, can anybody on the panel tell us if the pornographers are making money by putting these pornographic files on the file sharing programs?

Mr. SAAF. They are not directly making money, but a lot of pornography companies do put their files on the peer-to-peer network and mis-name it to try to gain exposure for the same purpose of advertising.

Mr. WAXMAN. Mr. Rung, I have heard that there is almost like a frequent flyer program; if you use a file sharing more often, you get access to more files and speedier access. Is that accurate?

Mr. RUNG. Not that I am aware of; what you might be referring to is a new feature that KaZaA came out with, a few months back, where the more you share, in theory, the higher rank you are for downloading from other people. We do not have a feature like that on our program.

Mr. WAXMAN. And why would they have a feature like that? Who benefits; does the file sharing operation benefit?

Mr. RUNG. I would assume that they would benefit, from the standpoint of the more the users used the program, the more ads that can be shown.

Mr. WAXMAN. Ms. Koontz, the GAO did a report for us, and we very much appreciate it. A lot of what is going on in these file sharing programs is illegal pornography. What is the problem? Why can law enforcement not find out who is putting the pornography on the files and getting them to the kids, and crack down on it?

Ms. KOONTZ. Well, I think, to a large extent, law enforcement has many, many efforts, and I am sure Mr. Netherland could add to this significantly.

But law enforcement has many efforts to identify individual users, determine their identity, to prosecute them in courts; and I am sure that he could probably add to this quite a bit in terms of the some of the difficulties in doing this and some of the barriers that they face.

Mr. WAXMAN. Well, maybe we ought to have him respond and give us some information on this point.

Mr. NETHERLAND. With respect to that, there are hundreds of thousands of images that exist on the Internet presently. As far as file sharing itself, it is just simply another vehicle by which these people can trade the material. With our Child Victim Identification Program, we are trying to quantify what the universe of images is out there, in hopes that we can locate these children that are being victimized; and also, when we run across a new image, we are going to hopefully be able to localize the source of that image, and back-track and locate the people that are, in fact, putting the stuff on the Internet.

Of course, with today's technology, digital cameras and so on, it is very easy simply to snap a photo and have it on the Internet within a matter of moments.

Mr. WAXMAN. What do the pornographers get out of doing this? How do they make money out of it?

Mr. NETHERLAND. The pedophiles, themselves, are gratified by the images. It arouses them sexually, and sometimes it ultimately leads to their actual molestation of a child. With respect to the people that are looking to make money on it, generally, they are, in fact, pedophiles, as well.

As far as peer-to-peer is concerned, it is exposure to the images. They, in turn, can point these people back to Web sites and so on that, in fact, do make money from this trade.

Mr. WAXMAN. Is it a failure of resources, insufficient resources; what is the barrier; or is it technological that keeps you from finding the people that are responsible?

Mr. NETHERLAND. Well, with respect to the CyberSmuggling Center, I have 13 people that are dedicated to the child exploitation effort at the CyberSmuggling Center.

Now our agents out in the field are also trained to conduct these types of investigations. However, simply because of the enormous number of tips that we receive on a daily basis, our posture is primarily reactive in nature.

Working peer-to-peer type cases is a proactive approach. I would like nothing more than to expand our efforts in that area, but we cannot ignore the massive number of tips that we are receiving already.

Mr. WAXMAN. Thank you, Mr. Chairman.

Mr. SHAYS [presiding]. I thank the gentleman. This is an amazing issue. Mrs. Miller.

Mrs. MILLER. Thank you, Mr. Chairman.

I will tell you, my daughter is 27 years old, so we did not really have the Internet in our home with some of these things. You know, the Internet really is quite a relatively new phenomenon.

I sit on a board in my county called Care House, which is for sexually abused children. It is unbelievable what people will do to their children.

As we are talking today about child pornography, as well, my husband has been the presiding Circuit Court Judge in our county for the family law and, again, you see it all.

When you do psychological profiles of these individuals, so often, pornography and access to pornography is a critical component to all of those kinds of things.

So I am just wondering, we talked a little bit about the marketing. The unfortunate reality is, quite frankly, there is a market for these kinds of things.

With teenagers today, how we can actually protect them from that? It seems to me as you see many of the law enforcement agencies who are having new Internet crime units, and I know we see that in my region and I am sure throughout the Nation as well, they are having some success with these things.

But I think it is difficult for us sometimes to legislate, because it seems as though the moment you pass a piece of legislation, the techies have out-thought you, again. So I guess I am looking a little bit more for specific recommendations on what you might think the Federal Government could actually do to assist in this regard.

Mr. SAAF. I think that local city government officials should take a more active stance on this approach. I am not sure that there is a broad sweeping Federal solution to this. But there are a lot of existing child pornography laws that are not being enforced by District Attorneys across the Nation.

I think that is really the first step, that it has to start at that level, and then we will see where it goes from there.

Mrs. MILLER. Thank you.

Mr. SHAYS. Thank you; Ms. Ruppersberger.

Mr. RUPPERSBERGER. Thank you, Mr. Chairman.

First thing, you wonder if we will be able to stay ahead of the technology to provide filters or for parental-type of controls.

But the issue is, whose obligation is it, in your opinion, to prevent the children from seeing this porn? Is it the software developers; is it the parent? Do you have an opinion on the obligation?

Because we have really allowed the industry to police itself for a long time, and there have been some positives and negatives. This is a time, I think, when the industry has not really stepped up. Does anybody want to take that question? Mr. Rung.

Mr. RUNG. As it was pointed out, the technology can change so quickly, that I think just outlawing this, or trying to regulate this, that, or the other thing, the technology would outgrow it almost immediately.

I really believe honestly that it is the parents that are the primary ones that are in the hot seat and have to, again, monitor their children's usage and monitor what goes on the computer.

Mr. RUPPERSBERGER. But do you not think the industry is better suited to come up with the evolving technology? I mean, there are a lot of parents that just cannot stay there at all times with their children.

There have to be some safeguards. There has to be, I think, an emphasis from the industry itself to help address this problem. I mean, law enforcement has to be involved. A lot of people have to be involved. Because if the industry does not step up, eventually Government will have to step up, and we will have to mandate.

Let me ask you this. Do you feel that the Government should mandate filters for the peer-to-peer networks? I know Dr. Greenfield does. Do you?

Mr. RUNG. To be quite honest, personally, I am against a lot of Government regulation in any case. But that would seem like, if you were going to do some regulation, that might be a worthwhile way to go about it.

Mr. RUPPERSBERGER. And if we do this and the technology keeps changing, there it gets back to the obligation end of the industry.

Another issue, too, as far as law enforcement is concerned, you mentioned the issue of local law enforcement. Whenever there is a problem with crime and there is a magnitude, I think it is very important for the Federal, State, and local governments to work closely together.

It seems that a lot of information leads come from local government, because that is where the every day operations is, that is what is happening in the street, in the communities.

What type of effort is evolving now to deal with this issue with respect to Federal, State, and local government? The prosecutor is the end. It needs to really be developed to obtain the information, get the intelligence, make the arrest, and then go to court and prosecute.

Mr. NETHERLAND. With respect to cooperative efforts, this particular area of crime is one area where we, law enforcement, work very, very well together. Both Federal, State, local law enforcement, as well as our international partners, are dedicated to this effort. We put aside our differences when we work these type cases.

The Internet Crimes Against Children Task Forces that exist out there, I think there are 36, I believe, now. They are comprised of Federal, State, and local law enforcement officers, and are one step in the right direction.

On the international level, we work very well with Interpol in France, as far as educating other countries on how to conduct these types of investigations. But right now, about 99 percent of this type of work is facilitated, quite frankly, by the Internet.

And if I could make one comment about the peer-to-peer file sharing filters and so on, that is certainly very important. I am a father, as well, and it is very important. It is a very important thing and we, as parents, have an obligation to take care of our children, and filter what they look at.

But keep in mind that this is still a vehicle by which these pedophiles can trade between themselves which, in turn, satisfies or arouses them, which ultimately and directly leads them to finding these children that are on the Internet and other areas, such as chatrooms and so on.

Mr. RUPPERSBERGER. I have one last question for Mr. Rung, again. I do not mean to keep picking on you, but you are the industry, I guess.

Have you or anyone that you are aware of in the industry contacted law enforcement agencies to try to work with them to try to identify where these problems exist?

Mr. RUNG. All I can speak to is what Grokster's experience is. We have corroborated in the past on some cases with law enforcement, and anticipate doing so in the future.

Mr. RUPPERSBERGER. But I am talking about taking the initiative. I am not talking about just cooperating when they come to you. Are you aware of the industry taking the initiative, when you have identified these problems, to help law enforcement?

Mr. RUNG. I do not believe there is any industry-wide. That is certainly a good idea.

Mr. RUPPERSBERGER. It is something that I think the industry needs to look at; because, if not, then Government will probably have to come in and mandate to deal with this serious problem. Thank you.

Mr. NETHERLAND. Thank you.

Chairman TOM DAVIS [presiding]. Thank you very much.

Mr. Janklow.

Mr. JANKLOW. Thank you very much.

Mr. Rung, if I could just continue for a moment, you corroborate, and I do not mean to say this in an accusatory way. I sound that way sometimes, but it is just the way I talk. I do not mean it that way.

You corroborate, but in your testimony, you say it is estimated that 50 percent of the files on files traded on sharing programs are pornographic, and you operate a file sharing program.

Now do you really feel your only responsibility is just to cooperate when you are contacted? For all practical purposes, you are the pornographer, when it comes to these types of things. You are the vehicle by which people are doing these things, and you cannot have Government shutting down everything and regulating everything all the time.

Do you feel there is a greater responsibility on the industry to step forward with something that is this obvious in preying against children?

Mr. RUNG. Let me address that two ways, if I could. The first is that the extent of the pornography on file sharing is just a sub-set of what is available on the Internet, as a whole, just as you pointed out.

Mr. JANKLOW. And I am going to get to that in just a second.

Mr. RUNG. Oh, OK, and so accordingly, it is there and it exists.

Mr. JANKLOW. Right.

Mr. RUNG. But the one thing that has occurred, this has been a learning experience for me, also, to be invited here and to listen to everybody here.

It is quite clear to me that it would make a lot of sense for me to go back to my fellow entrepreneurs in our industry, and see what we can, in fact, do on a pro-active basis.

Mr. JANKLOW. Does it take a congressional hearing to let you know there is problem of this magnitude?

Mr. RUNG. Of this magnitude, yes, particularly with the child pornography.

Mr. JANKLOW. Sir, you brought up another point. The mis-spelling of words is not a file sharing issue. But everybody wants to say "parental involvement." This is one where it cannot be just the parents, primarily. Kids go to school. We all bust our tails to make sure our schools have more computers all the time for the kids.

We have community libraries that have computers. Kids go to their neighbors' houses, where there are computers. They go to church, where there are computers, and boys and girls centers, where there are computers. So it is not just a matter of dealing with their parents.

If the University of New Hampshire's study is accurate, only 10 percent of the students that are hit on, on the Internet, tell their parents about it.

Even though you have a warm, fuzzy relationship with your parents, you may be bashful or embarrassed with this bestiality that you see, the sodomy that you see.

You know exactly what I am talking about. You can misspell words and get it. You can innocently stumble into, like, we all say, whitehouse.com is a good example of that.

But my question is, sir, what do you think it is going to take to better protect the children of the world, recognizing that we cannot just pass laws in America? A lot of these sites come from outside the United States. They are just as easy to come from Bulgaria or Romania, as they are South Dakota or Timbuctoo, AR.

Mr. RUNG. I honestly have no solution to that.

Mr. JANKLOW. Mr. Netherland, how about you? Do you agree there is not enough money in the world, just to prosecute, after these children are exposed to this type of thing; that we have to really do something at the front end, and your organization is just dealing with our failure as a society to deal with it on the front end?

Mr. NETHERLAND. As far as law enforcement is concerned, I welcome any strengthening of the laws that help us do our job better, and that would remove these people from doing what they do.

Mr. JANKLOW. Sir, is your agency involved in the Justice Department funding of those Internet Crimes Against Children Programs?

Mr. NETHERLAND. We have an advisory role with respect to the Internet Crimes Against Children Task Forces.

Mr. JANKLOW. Do you know of any reason; is it a shortage of money; what is it that has prevented all 50 States and the territories from getting funding to get these things launched?

My State happened to have been the first Statewide program. We were lucky to get in on the funding. But what does it take? Is it a funding issue, to make sure that every Government has the opportunity to get together to do this?

Mr. NETHERLAND. I believe that it would certainly help, in terms of making sure that every single State has an Internet Crimes Against Children Task Force, and organizes one. Because this is across the Nation; it is across the globe.

Mr. JANKLOW. And sir, I will say that this is one of those issues where the Federal Government, the Federal prosecutors have truly stepped up to the plate, and have really dealt with it, when the evidence is turned over to them with respect to these predators.

I have one other question for Ms. Koontz. What is it that you think that Congress can do, if anything, to really try and assist in shutting this off?

When I was a kid, it was National Geographic. But that is a lot different than what is going on out there today. These sites have a huge impression on 8, 9, 10, and 11 year olds; a huge impression.

Unfortunately, we did not put that kind of thing up today, and I guess my time is up. But could you tell me, do you know of anything that we could do?

Ms. KOONTZ. This is not the kind of problem, I think, that lends itself to sort of a single legislative solution. I think, though, it needs to be a combination of efforts.

First and foremost, law enforcement needs to continue to follow-up on the tips that they receive in this area, and they need to have the resources in order to further investigate those.

This is a very growing area. The tips in the peer-to-peer networking area increased fourfold in 1 year. So you can tell this is very much on the rise.

But the reality of it is, I think in addition to what law enforcement and public policy could do, is some of the things that other people on the panel have mentioned.

Those are educational strategies for our kids. It is parental involvement and supervision, and although they are generally imperfect, technology-based tools, such as the ones Dr. Greenfield mentioned that are actually on KaZaA, can be a legitimate part of an overall strategy for dealing with this.

Mr. JANKLOW. Thank you.

Chairman TOM DAVIS. Thank you very much.

Mr. Putnam.

Mr. PUTNAM. Thank you, Mr. Chairman.

I share Governor Janklow's frustration about this, and particularly, really, the inability for anybody to get their arms around a solution.

I had a constituent of mine, who was a young woman, who experienced the same thing. She wandered off onto the Internet. She met someone and was lured away to Greece. She was severely molested for a period of several months, before anyone could track her down.

The local law enforcement received almost no help from the Federal Government. The FBI was not interested. No one was interested until they finally managed to find a postcard that he had mailed her, and a Postal Inspector was the only Federal law enforcement help they got.

We have a rating system for video games. We have a rating system for movies. We have a rating system for music, and the panels consensus is that people who deliberately set up Web sites to prey on spelling errors of third graders looking at Pokemon is not something that we can have the collective wisdom or will to solve. I have a problem with that. I think that there is a way that we can get around that.

But I want to know a couple of things. First of all, because of what was mentioned about the resort in Acapulco, how much of this is generated domestically versus internationally? Is there a list maintained by the State Department, or someone of nations who continue to prey on children, and whose legal system does not allow us to get the information or the help that we need to prosecute these folks?

The chairman and Mr. Waxman put out a helpful handout for parents. But the question I would ask the panel is, for the "do-good parent" whose child brings some of these things to their attention, and they scan down, and you see all of these terms: co-ed, teen, young girl, cheerleader, all things that clearly indicate a minor, at what point does it go from smut to being illegal smut?

How does the average parent know what they can report, and what things are just in bad taste but do not cross the line of illegality? So those are a handful of questions. I will leave it to the panel to decide who is most appropriate to answer.

Mr. NETHERLAND. With respect to the case in Acapulco, and also the case with Operation Hamlet, the Bureau of Immigration Customs Enforcement approaches things on an international level. We look at material that is crossing the borders into the United States. Unfortunately, the United States is the largest consumer of this type of material. I think that is a well known fact.

Mr. PUTNAM. Who is the largest producer? Is that the United States, also?

Mr. NETHERLAND. In my opinion, there is a lot of material that is produced in the United States. But I believe there are many countries out there who, because of their laws, do not outlaw the possession of child pornography, or large producers; Russia, for instance.

I know that they are taking steps to address that issue, and we work closely with the Russian authorities on investigations. But it is a function of their laws, trying to deal with the problem, themselves. In South America, some of the countries here also have some issues.

Mr. PUTNAM. Help me understand this. Let us stop right there, because I guess I gave everybody too much to chew on. Help me understand what is against the law. At what point is changing the "e" to an "a" in Britney, and putting up pictures of children engaged in sexual acts against the law?

At what point is changing Pokemon or Schwinn bicycles or whatever for the specific purpose of bringing in young children to this realm against the law; MediaDefender?

Mr. SAAF. Well, that is kind of big opinion question because, you know, if something gets thrown up on the peer-to-peer network and it is given a name, the person in the image might look 16. They might be 19.

It is impossible to know, because these are just digital replications that have occurred millions of times over on the network, and you do not know where it started from. So who is to say if it is against the law or not? That is the real difficulty of peer-to-peer networking.

Mr. PUTNAM. Mr. Rung.

Mr. RUNG. I am not sure. I was interested to hear the actual answer to that myself. Because I am not sure of what the legal definition of what is considered child pornography or not is. I mean, obviously, if you have a 6-year-old girl in an image, then that is a potential problem. So I am actually quite interested in the answer, myself.

Mr. PUTNAM. So advertising hot high school cheerleader coeds, currently there is no law against that, if the image is actually someone over the age of 18?

Mr. NETHERLAND. That is correct.

Mr. PUTNAM. And there is no trademark or copyright protection because of the fact that it is misspelled. But there is also no intent; there are no conspiracy laws that would apply to that.

I mean, Mr. Waxman has made a career out of the intent or the conspiracy of advertising of certain products in this country. I find it hard to believe that you could not extrapolate that type of a legal argument to include changing the spelling of Pokemon to lure children into child pornography. Is there no remedy there, either; Ms. Koontz?

Ms. KOONTZ. I guess what I would add here is that it is not necessary for the user to misspell Pokemon or Britney, or any of the rest of them to have pornography and child pornography return to your computer.

It is not so much of an issue of, shall we say, the mis-labeling of files. It is much more a function of the types of files being kept by individual users, who now have the capacity, through the file sharing applications to locate and interact with each other directly. These are individuals who are doing this, and they are just sharing what they possess on their hard drives.

Chairman TOM DAVIS. Thank you.

Ms. GREENFIELD. Could I say something about that? Just to add to that, a lot of it, therefore, is what young people themselves have downloaded. It is not just outsiders preying on kids. It is also what kids are creating for themselves. So that is a very, very important part of the problem, which needs to be also addressed.

Chairman TOM DAVIS. Thank you; Mr. Tierney.

Mr. TIERNEY. Thank you, Mr. Chairman; Mr. Chairman, I would like to yield to Congressman Waxman, who has a question.

Mr. WAXMAN. I thank you for yielding, because I want to follow-up on the points that have just been raised. It is difficult to find out what criminal laws are broken. But one key thing would be to find the end user.

And if MediaDefender can identify the IP address of people offering child porn, why has anyone not asked the ISP to turn over the names of the end users? Is that impossible to do, for any reason?

Mr. SAAF. Well, MediaDefenders tried to encourage law enforcement officials, and we have had very low success. There have been a few District Attorneys around the country that have taken interest in this.

I have a list right here that I collected over 2 days, of 300,000 IPs that I believe have something to do with child pornography, at least by their facial terminology, and I would be happy to turn that over, but who do I turn it over to? I really do not know.

Mr. NETHERLAND. I can say that with respect to tracking these individuals back to the person opposed to damages, the files, and I will not discuss exactly what our techniques are, but we have a means by which we can backtrack and locate those individuals.

We do, in fact, do that. We look for persons who are posting multiple files, hundreds of images. So we do have a means to do that.

Mr. WAXMAN. Do you get the cooperation of the ISP, Internet Service Provider, to do that?

Mr. NETHERLAND. Yes, sir, we do.

Mr. WAXMAN. And there is a problem in getting their cooperation?

Mr. NETHERLAND. Correct; the point here is that in these type applications, there is no centralized location; there is no centralized ISP that can report this.

This particular network is simply, each desktop computer, in and of itself, is a server. So you have to locate the end user or the poster, in order to shut it down.

Mr. WAXMAN. Thank you; I thank the gentleman for yielding, because that was a point I thought we would need to clarify.

Mr. TIERNEY. Thank you; I yield back the balance of my time.

Chairman TOM DAVIS. Thank you very much; Mr. Shays.

Mr. SHAYS. Thank you, Mr. Chairman; Mr. Chairman, thank you for having these hearings. Mr. Waxman, thank you for the good work you and your staff have done on this, as well.

This may sound a little crazy, but bear with me a second. I want quick answers, and I want to go all the way down the line. Ms. Koontz, I want to know who are the bad guys.

Ms. KOONTZ. The pornographers.

Mr. SHAYS. I want you to be a little bit more specific; just the pornographers?

Ms. KOONTZ. Yes.

Mr. SHAYS. Mr. Netherland.

Mr. NETHERLAND. I believe the pedophile drives the market. They drive the market. They are the ones preying on our children, and they use whatever vehicle they have by which to do so.

Mr. SHAYS. Well, I think there are two kinds of bad guys with regard to peer-to-peer networks. There is the original pedophile, who creates the information and originally posts it to the network. That guy is the bad guy.

But let us face it, there is a huge demand; 300,000 people is a huge group of people. That means there is a lot of mid-level, borderline pedophiles, who have a fleeting interest in this stuff enough to download it and maybe even accidently re-share it.

So I do not know if you want to necessarily put that in the same moral evil as the guy who originally creates this stuff, but it is definitely a lot of people. Probably you would be surprised. I mean, clearly, there is a bunch of people in the Government who are the bad guys, to some degree.

Mr. SHAYS. And in the sense of the Government, quickly, who would that be?

Mr. NETHERLAND. Well, like I said, NASA, Department of Defense, Los Alamos National Laboratory. I could give you another couple hundred computers that are all tracked down. You could identify every one of those computers to an owner of that computer, someone that works at the Government, who has a file that appears to be child pornography.

Mr. SHAYS. Mr. Rung.

Mr. RUNG. I would say the creators of the child porn and the consumers of the child porn.

Mr. SHAYS. A little louder, please; the creators of child porn and who else?

Mr. RUNG. The creators of the child porn and the people that consumer it. That would be the people that download it.

Mr. SHAYS. Would you consider yourself one of the bad guys?

Mr. RUNG. No, I do not believe so.

Mr. SHAYS. Dr. Greenfield.

Ms. GREENFIELD. That is a very hard question. But I think I would probably go with Mr. Rung's answer.

Mr. SHAYS. Would any of you consider Mr. Rung one of the bad guys?

Ms. GREENFIELD. Well, I feel like we should not pick out peer file sharing; that this is a problem throughout society. It is a problem on television. It is a problem throughout the Internet. It is a problem when you go now to checkout at the supermarket, with what used to be very innocent women's magazines. The banner headlines all over the covers now are all about sex.

So I think that throughout society, and I could even get closer to home, there has been a highly sexualized environment, and that is a problem. But I do not really see one bad guy.

Mr. SHAYS. Mr. Rung, I am starting from the bottom here, just to try to understand something. In your terms of agreement, you prohibit the use of your service in transmitting any content that is "unlawful, harmful, threatening, abusive, vulgar, obscene, or otherwise objectionable." But is that not kind of a joke?

Mr. RUNG. If you mean from the standpoint, is it enforceable by anything that we can do? That is correct, we cannot enforce that.

Mr. SHAYS. So what do those words mean to us? I mean, are they to protect yourself from legal action? What is the purpose of your terms of agreement?

Mr. RUNG. I think it is two-fold. One is to provide protection; let us be honest. But the second is to put our users on notice that this not the type of activity that you should engage in, with the product that we provide.

Mr. SHAYS. How much of your income would you say is attributed to the very topic that we are discussing now? By the way, I appreciate your honesty. You are helping me understand this issue better than most people have. So it is good you are here and thank you. I am just trying to understand it. But how much of your income would it be?

Mr. RUNG. No, that is fine and I appreciate that. I have learned a lot coming here too and, as a matter of fact, I would like to spend a little time with Mr. Netherlands after the meeting.

Mr. SHAYS. Thank you.

Mr. RUNG. But again, I really do not know the percentage of child porn that goes through by the users. But I believe it is relatively small, compared to the universe of files that are shared.

Mr. SHAYS. Would you come back to the committee and give us a more specific answer to the question of how much of your income you believe is the result of stuff like what we are talking about?

Mr. RUNG. Yes.

Ms. GREENFIELD. One thing I think could be done by the companies themselves would be not to sell banner ads for things like condoms. Because those are under their control, and they are something that children or anybody else cannot avoid when they come onto the site.

Mr. SHAYS. Thank you, Mr. Chairman, and thank you.

Chairman TOM DAVIS. Are there any other questions; Mr. Van Hollen.

Mr. VAN HOLLEN. No, and Mr. Chairman, I want to thank you for holding this hearing. I am still trying to master the art of being in two places at one time. I was at another committee hearing.

I want to thank Congressman Waxman and his staff for what they have done. As the father of three children 12 and under, this is something that I have a great interest in.

I have been looking through some of the recommendations. One of the big frustrations, of course, is trying to come up with concrete measures we can take. Obviously, education, and public education, and making sure parents are alert is a critical part of this.

But I am going to look through this to see if you have any other specific recommendation. Law enforcement is a key part. But are there other tools we can use, and I realize how difficult it is in the Internet age, to keep these kind of things from popping up when you put in "Pokemon." It is incredible, and as much as we monitor our kids, it is impossible to be there 24 hours a day, standing in front of the computer.

But I look forward to reviewing some of the recommendations and hearing more about this. Thank you.

Chairman TOM DAVIS. Thank you very much; and Mr. Waxman, let me thank your staff, too, for helping in calling this to our attention and doing the work on this. I think this was a very useful hearing.

I want to thank all of our witnesses for attending. I think for Members, we have learned a lot today, and we will go back and probably re-visit the issue. If any other thoughts occur to you, please feel free to let the committee know, and we will be happy to put it in the public record.

We will be posting on our Web site a list of the top 10 things a parent can do to limit their children's exposure to pornography on peer-to-peer file sharing networks, compiled by Mr. Waxman's staff and mine, and we will also be following-up on this issue.

In addition to the pornography problems, file sharing programs raise serious security and privacy issues, as users may unknowingly share personal files, or may accidently download files computer viruses.

Thank you very much. The hearing is adjourned.

[Whereupon, at 11:40 a.m., the committee was adjourned, to reconvene at the call of the Chair.]

[Additional information submitted for the hearing record follows:]

PARENTAL TIPS FOR INTERNET FILE-SHARING PROGRAMS
REPS. TOM DAVIS AND HENRY A. WAXMAN
COMMITTEE ON GOVERNMENT REFORM
March 13, 2003

Popular Internet file-sharing programs like Kazaa, Morpheus, and Grokster make millions of pornographic images and videos available to teenagers at the click of a mouse. Here are some guidelines to help concerned parents address this serious problem:

- **Recognize the Danger.** Two of every five children between the ages of 12 and 18 have used file-sharing programs to download music, but their parents may not realize that these programs also operate like a vast free library of digital pornography. One way to learn more -- and to open a dialogue -- is to ask your child what he or she knows about the programs and whether he or she has encountered pornographic content.

- **Communicate.** Research indicates that children who discuss issues with their parents are less likely to engage in risky behaviors. Look for opportunities raised in the news media, movies, or school events to discuss Internet use and file-sharing programs.

- **Reduce Opportunities for Misuse.** Consider strategies such as locating the computer in a common area and having regular shared Internet sessions. Many teenagers will understand that reasonable parental oversight helps reduce the temptation to use the computer to explore inappropriate content.

- **Don't Rely Too Much on Parental Filters.** There is no fool-proof technological "fix" to the parental issues raised by the Internet. In fact, the current versions of many of the most popular filters don't filter pornography on file-sharing programs. While some programs do allow parents to block file sharing altogether, these options generally are not automatic. Parents wishing to use these products should be sure they are properly configured.

- **Recognize Early Signs of Trouble.** If parents are concerned about their children's use of the Internet, they should immediately increase supervision and, if necessary, seek assistance from professionals.

For more information, here are some web sites that may be of help: SafeKids.com (http://www.safekids.com); GetNetWise (www.getnetwise.org); NetSmartz (www.netsmartz.org).

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

CHILDREN'S EXPOSURE TO PORNOGRAPHY ON PEER-TO-PEER NETWORKS

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 General Accounting Office and the staff of the Government Reform Committee investigated a new challenge facing parents of children growing up in the digital age: the widespread prevalence of pornography on peer-to-peer networks accessed through file-sharing programs. This report summarizes the GAO findings and describes the results of the congressional staff investigation.

File-sharing programs are popular Internet applications that allow users to download and share electronic files apart from the World Wide Web. The first such program, Napster, was used by as many as 1.6 million people simultaneously. Since Napster was shut down by court order, newer file-sharing programs have surged in popularity and have become one of the most popular uses of Internet technology. One of the most popular current file-sharing programs, Kazaa, typically has four million simultaneous users. Other popular file-sharing programs include Morpheus, iMesh, BearShare, LimeWire, and Grokster.

Parents are often unaware of how these file-sharing programs operate and what risks they pose to their children. Almost all news coverage of file-sharing focuses on the ability of users to trade copyrighted music and movies. This report examines a darker side of these new programs: the risk they pose to children of being exposed to pornography. The report finds:

- **Pornography is widely available on peer-to-peer networks accessed through file-sharing programs.** File-sharing programs operate like a vast digital library available without charge to users. The pornographic section of this library, which children can freely access, is enormous. Nearly six million video, image, and other files identified as "xxx," "porn," or "sex" were available for downloading on just one popular peer-to-peer network in a recent two-day period. Moreover, GAO found that there is easy access to illegal child pornography via file-sharing programs.

- **Children using file-sharing technology can be exposed inadvertently to pornographic content.** After searching for "Britney," "Pokemon," and "Olsen twins," GAO found that more than half of the files it retrieved were pornographic, including 8% with child pornography or child erotica.

- **Parental tools to prevent children's exposure to pornography on peer-to-peer networks have limitations.** Many parents rely on parental control software like Net Nanny or Cyber Patrol to limit their children's access to online pornography. Although some of these programs can be configured to block any access to file-sharing programs, they generally do not have the capacity to allow access to file-sharing programs while filtering out pornographic files. Settings exist on popular file-sharing programs to reduce inadvertent exposure to pornography, but these can be circumvented.

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 networking — to trade music files. At its peak in February 2001, Napster had as many as 1.6 million simultaneous users.[1]

How does file-sharing work?

Peer-to-peer (P2P) file sharing is a direct connection between two users' computers over the Internet. Using file-swapping software, a user shares selected contents of his or her hard drive with other users. To find a file, you use P2P software to search others' drives, make a direct connection to another user, and download the file from their machine.

Source: CNET.com

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.

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

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 music content. And whereas the Napster network was centralized around one computer server which tracked the trade of files, these new programs allow direct user-to-user file trading.

The new file-sharing programs include programs like 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 almost 400 million times. Kazaa, the most popular file-sharing program, has been downloaded more than 199 million times. It is currently the most popular download on Download.com, a software clearinghouse.[2] *See* Table 1.

Table 1
Downloads of Popular File-Sharing Program

File-Sharing Program	Total Downloads	Weekly Downloads
Kazaa	199,981,000	3,025,000
Morpheus	109,846,000	194,000
iMesh	45,378,000	436,000
BearShare	18,137,000	18,000
LimeWire	15,233,000	10,000
Grokster	7,091,000	102,000

Source: 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 million users

[2] Online at http://download.com.com/3101-2001-0-1.html?tag=dir.

connected to the network simultaneously — two and a half times the number of users Napster had at its peak.[3] *See* Figure 1.

Many of the users of these new file-sharing programs are under the age of 18. Research done by Peter D. Hart Research Associates for the Recording Industry Association of America has found that of those who download files through file-sharing programs, 41% are

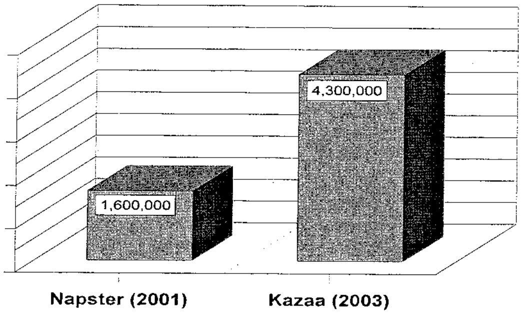
File-Sharing and Universities

The popularity of file-sharing programs among young people is causing problems at colleges and universities. Northwestern University reports that, at times, nearly 100% of its bandwidth is being used by file-sharing programs. The University of California at Berkeley has capped bandwidth usage and, according to the school newspaper, "The popularity of newer file-sharing programs . . . (has) been blamed for the network slowdown."

- *NU pressured to crack down on file sharing on computers,* Daily Northwestern (Oct. 25, 2002).

- *Bandwidth Capped for Dorm Residents,* Daily Californian (Oct. 5, 2001) (online at www.dailycal.org/article.asp?id=6538).

Figure 1
Simultaneous Users of the Most Popular File-Sharing Programs



Source: *Neo-Napsters Proliferate in the Wake of Napster's Demise,* Broadband Week (Aug. 2001). On February 5, 2003, at 3:00 p.m., Kazaa indicated 4,339,000 concurrent users.

[3] On February 5, 2003, at 3:00 p.m., Kazaa had 4,339,000 concurrent users.

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]

The Purpose of This Report

Although file-sharing is enormously popular among digitally connected youth, the public at large is unfamiliar with these programs. Almost all news coverage of file-sharing focuses on just one issue: the ability of users to trade copyrighted music, movies, and videos. As a result, many parents who know about these technologies view copyright concerns as the only major issue these programs raise.

The content available through file-sharing programs is not limited to copyrighted music and motion pictures, however. It also includes graphic pornography. When searching the Web, children are somewhat shielded from the most hardcore pornography by the need to use a credit card to pay for access. But on file-sharing programs, even the most offensive content, including illegal child pornography, is available for free. This raises new and difficult issues for parents.

Reps. Tom Davis and Henry A. Waxman, the Chairman and Ranking Member of the Committee on Government Reform, requested this report and a companion report by the General Accounting Office to examine the prevalence of pornography on peer-to-peer networks and the issues they raise for parents. These reports are a followup to a report on this issue released by Rep. Waxman and Rep. Steve Largent in July 2001.[6]

[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).

[6] Committee on Government Reform Minority Staff Report, *Children's Access to Pornography through File-Sharing Programs* (July 27, 2001).

The GAO investigation examined three questions:

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.
3. The extent of federal law enforcement resources available for combating child pornography on peer-to-peer networks.

This report provides additional information about the quantity and popularity of pornography on peer-to-peer networks. It also assesses the ability of parental control programs like Net Nanny, Cyber Patrol, and others to block pornographic content on peer-to-peer networks.

FINDINGS

Pornography Is Widely Available on Peer-to-Peer Networks

There is no published data on the quantity of pornographic material available through file-sharing programs. In response to an inquiry from the Committee, MediaDefender, a company with expertise in peer-to-peer networks, undertook an assessment of the amount of pornographic content that is available to children using these programs. MediaDefender searched for pornographic files available for downloading on the FastTrack network, which is the peer-to-peer network used by several popular file sharing programs, including Kazaa and Grokster. The search terms it used were words commonly associated with pornographic material.

KEY FINDINGS:

In one two-day period, there were almost six million pornographic files available for download on one peer-to-peer network.

The pornographic files available through peer-to-peer networks include many files containing child pornography.

For one two-day period, MediaDefender searched the networks for files containing the terms "porn," "xxx," or "sex" in their file names, titles, keywords, or descriptions. MediaDefender found almost six million files available for download that had a least one of these terms present.[7] If peer-to-peer networks are conceptualized as a digital library available for free downloading, MediaDefender found that the pornography section of this library makes nearly six million titles available to children and other users.

As part of its investigation, GAO looked specifically at the availability of illegal child pornography on peer-to-peer networks. Using 12 keywords known to be linked with child pornography, GAO found many files with names associated with child pornography images. With the assistance of the Customs Service CyberSmuggling Center, GAO analyzed 341 of the images it downloaded through Kazaa. Of these, nearly half were determined to be child pornography.

Searches for Entertainment Figures Popular with Children Yield Many Pornographic Files

Even if children are not searching for pornography on peer-to-peer networks, they are likely to be inundated with pornography as they use file-sharing programs. To assess the degree to which a young user might inadvertently access pornographic content while using file-sharing programs, GAO used the Kazaa program to search for files containing terms that a young user might try when looking for videos and images of entertainment figures popular among children. The specific terms used by GAO were "Britney," for popular female singer Britney Spears; "Olsen twins," popular child actors; and "Pokemon," a cartoon character popular among children.

KEY FINDING:

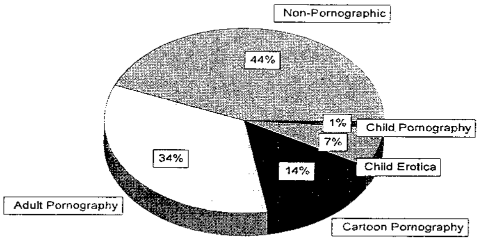
Of the images found using the search terms "Britney" "Olsen twins," and "Pokemon," more than half were pornographic.

[7] MediaDefender, original research conducted for the House Committee on Government Reform (Mar. 7, 2003).

Working with the Customs Service CyberSmuggling Center, GAO found that 56% of the files it retrieved contained pornographic or erotic content. Among the files retrieved by GAO, 34% contained adult pornography, 14% contained cartoon pornography, 7% contained child erotica, and 1% contained child pornography. *See* Figure 2.

Figure 2

Images Found Using Search Terms "Britney," "Olsen twins," and "Pokemon"

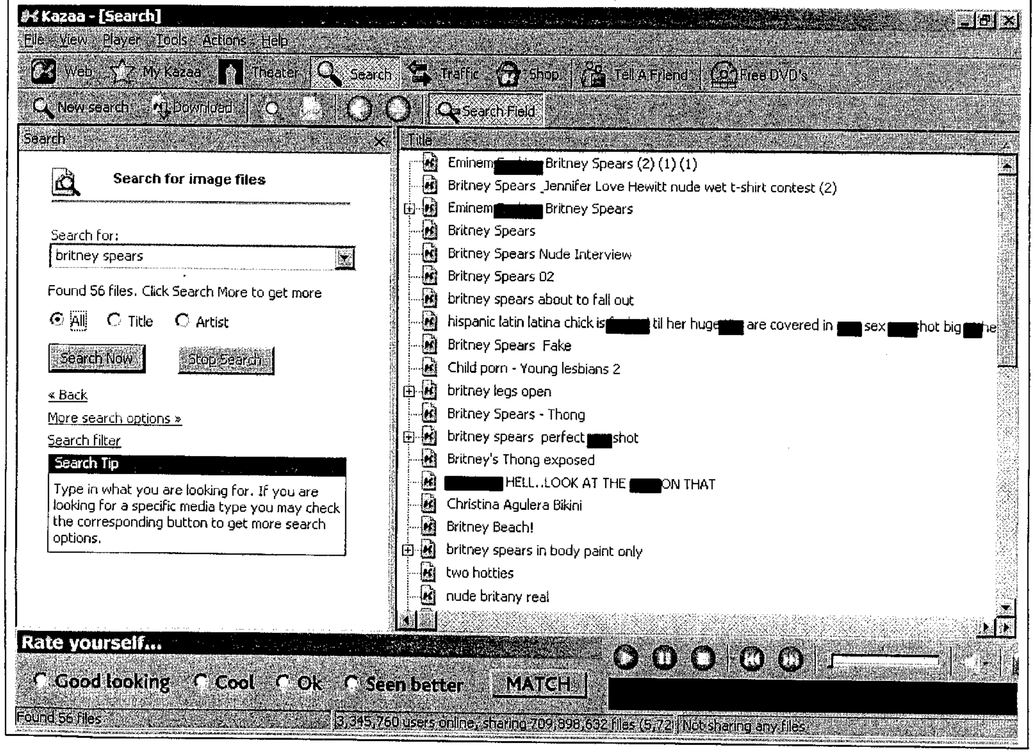


Source: GAO, *Peer-to-Peer Networks Provide Ready Access to Child Pornography* (Feb. 2003) (GAO-03-351).

Even the names of the files are often obscene or pornographic, containing references to graphic sexual content. These file names would be seen by a child even if he or she did not download or view the content of the files. Figures 3, 4, and 5 display the redacted results of recent searches performed by Committee staff for "Britney Spears," "Olsen twins," and "Pokemon."

Figure 3

Kazaa Search Results for "Britney Spears"



Search for image files

Search for: britney spears

Found 56 files. Click Search More to get more

● All ○ Title ○ Artist

Type in what you are looking for. If you are looking for a specific media type you may check the corresponding button to get more search options.

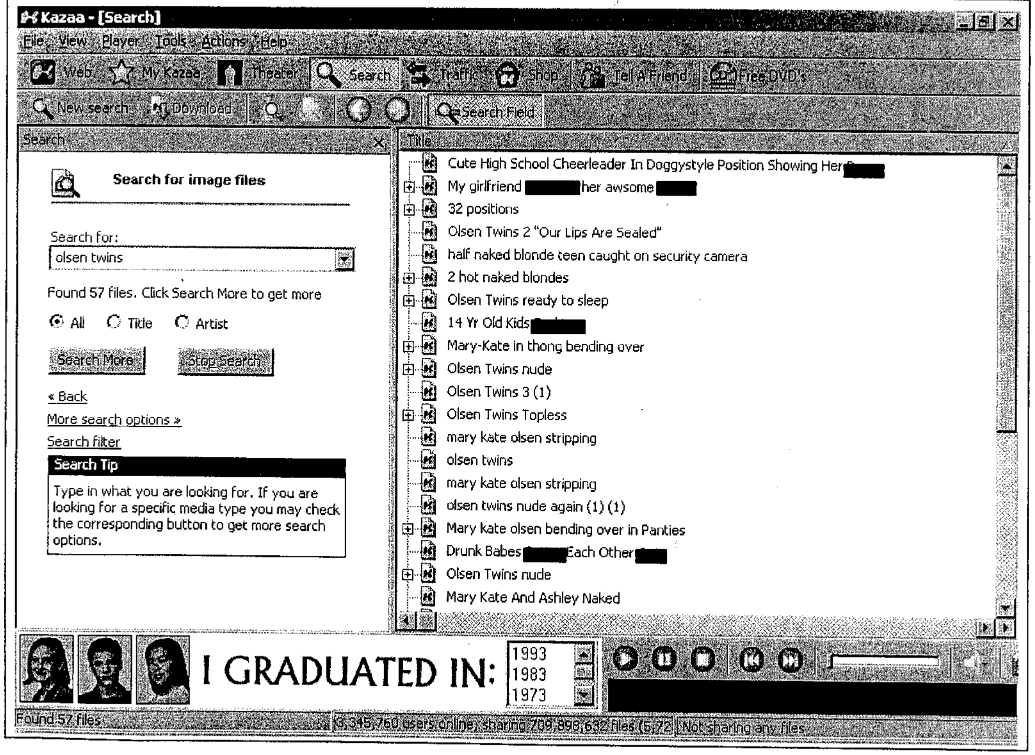
- Eminem[redacted]Britney Spears (2) (1) (1)
- Britney Spears Jennifer Love Hewitt nude wet t-shirt contest (2)
- Eminem[redacted]Britney Spears
- Britney Spears
- Britney Spears Nude Interview
- Britney Spears 02
- britney spears about to fall out
- hispanic latin latina chick is[redacted] til her hug[redacted] are covered in [redacted] sex[redacted]hot big[redacted]he
- Britney Spears Fake
- Child porn - Young lesbians 2
- britney legs open
- Britney Spears - Thong
- britney spears perfect[redacted]shot
- Britney's Thong exposed
- [redacted]HELL..LOOK AT THE [redacted]ON THAT
- Christina Agulera Bikini
- Britney Beach!
- britney spears in body paint only
- two hotties
- nude britany real

Found 56 files

3,345,760 users online, sharing 709,898,632 files (5,72 Not sharing any files

Figure 4

Kazaa Search Results for "olsen twins"



Kazaa - [Search]
File View Player Tools Actions Help
Web My Kazaa Theater Search Traffic Shop Tell A Friend Free DVD's
New search Download Search Field
Search
Title

Search for image files

Search for:
olsen twins

Found 57 files. Click Search More to get more

● All ○ Title ○ Artist

Search More | Stop Search

« Back
More search options »
Search filter

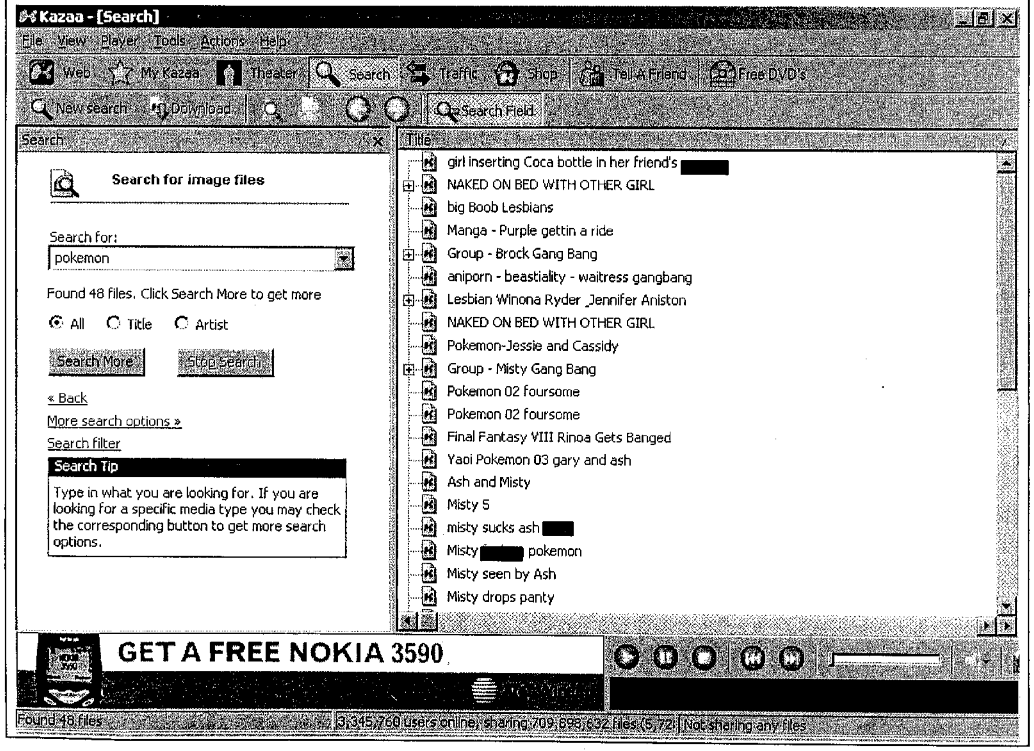
Search Tip
Type in what you are looking for. If you are looking for a specific media type you may check the corresponding button to get more search options.

Cute High School Cheerleader In Doggystyle Position Showing Her[redacted]
My girlfriend [redacted] her awsome [redacted]
32 positions
Olsen Twins 2 "Our Lips Are Sealed"
half naked blonde teen caught on security camera
2 hot naked blondes
Olsen Twins ready to sleep
14 Yr Old Kids[redacted]
Mary-Kate in thong bending over
Olsen Twins nude
Olsen Twins 3 (1)
Olsen Twins Topless
mary kate olsen stripping
olsen twins
mary kate olsen stripping
olsen twins nude again (1) (1)
Mary kate olsen bending over in Panties
Drunk Babes [redacted] Each Other [redacted]
Olsen Twins nude
Mary Kate And Ashley Naked

Found 57 files | 3,345,760 users online, sharing 709,898,632 files (5,72 | Not sharing any files

Figure 5

Kazaa Search Results for "Pokemon"



Search for image files

Search for:
pokemon

Found 48 files. Click Search More to get more

● All ○ Title ○ Artist

« Back
More search options »
Search filter

Search Tip
Type in what you are looking for. If you are looking for a specific media type you may check the corresponding button to get more search options.

girl inserting Coca bottle in her friend's [redacted]
NAKED ON BED WITH OTHER GIRL
big Boob Lesbians
Manga - Purple gettin a ride
Group - Brock Gang Bang
aniporn - beastiality - waitress gangbang
Lesbian Winona Ryder _Jennifer Aniston
NAKED ON BED WITH OTHER GIRL
Pokemon-Jessie and Cassidy
Group - Misty Gang Bang
Pokemon 02 foursome
Pokemon 02 foursome
Final Fantasy VIII Rinoa Gets Banged
Yaoi Pokemon 03 gary and ash
Ash and Misty
Misty 5
misty sucks ash [redacted]
Misty [redacted] pokemon
Misty seen by Ash
Misty drops panty

Found 48 files | 3,345,760 users online, sharing 709,898,632 files (5,72 | Not sharing any files

Parental Tools to Limit Children's Exposure and Access to Pornography on Peer-to-Peer Networks Have Limitations

Parents who are concerned about reducing their children's access to pornography online often use parental control software such as Net Nanny, Cyber Patrol, or McAfee Internet Security. But these programs have had limited effectiveness with file-sharing programs. The report released by Reps. Waxman and Largent in July 2001 assessed the ability of these programs to block pornographic content on peer-to-peer networks. That report found: "Popular parental filters do not block access to pornographic files through file-sharing programs."[8]

KEY FINDINGS:

Parental control software has limited ability to filter pornographic content accessed through file-sharing programs.

Settings in some file-sharing programs can reduce inadvertent exposure to pornography, but can be circumvented.

Since July 2001, all of the leading parental control software companies have released new versions of their popular titles. This report assesses the ability of these new versions to block pornographic content on peer-to-peer networks. The specific programs investigated are AOL Parental Controls, Cyber Sentinel, Cybersitter, Cyber Snoop, Cyber Patrol, McAfee Internet Security, Net Nanny, Norton Internet Security, and Zone Alarm Pro.

Most of the popular file-sharing programs also contain features designed to enable the user to block pornographic content. This report assesses their effectiveness as well.

Parental Control Software

The makers of parental filtering programs are becoming aware of parents' concerns regarding file-sharing. In an interview, Andrew Tull, an executive with BioNet Systems, makers of Net Nanny, said, "We listen to what our customers are talking about. Parents are just starting to become aware of P2P and what their

[8] Committee on Government Reform Minority Staff, note 6.

kids are looking at."[9] In general, however, these programs are still not able to filter out pornographic content found through file-sharing programs.

Parental control software was designed for use on the World Wide Web. The programs allow access to the Web, but block children from gaining access to sites offering pornography by restricting access based on both prohibited website addresses and keywords found on the sites.

These approaches do not automatically work with file-sharing programs. While file-sharing is an Internet technology, it is not browser based. Only one of the nine parental control software programs tested — Cyber Sentinel — allows parents to permit their children access to peer-to-peer networks while filtering out pornographic content. Cyber Sentinel is not a true filter, however, in that it responds to pornographic content by closing down the file-sharing program.

Several of the other programs reviewed in this report did offer options to block access completely to file-sharing programs. This is an "all or nothing" approach to access to peer-to-peer networks because it either allows unrestricted access or blocks children from using the programs for any purpose. In general, the programs using this approach required extra steps to configure the program and had functional limitations that might reduce their usefulness as parental tools.

One program — Cyber Patrol — allows parents to select programs that their children may not use. To use this feature, parents must select the blocked programs from those already installed on the computer. This approach requires that the parent monitor whether new programs have been downloaded and installed. Two other programs — Net Nanny and Zone Alarm Pro — can be configured by parents to block the most popular file-sharing programs. For newer and less common file-sharing programs, this approach requires parents to specify which programs to block.

One program — Cybersitter — can be configured to block some file sharing programs. However, Cybersitter can not easily be configured by the user to block the most popular file-sharing program, Kazaa. Committee staff succeeded in blocking Kazaa only after detailed consultation with Cybersitter's technical support.

[9] Telephone conversation with Andrew Tull, President of Sales and Marketing for BioNet Systems (Feb. 12, 2003).

Only two programs appeared to allow parents to restrict all access to file-sharing programs. McAfee Internet Security and Norton Internet Security provide the option to limit children's Internet access to specified programs (such as a web browser), making it impossible for them to use any other programs to connect to other users to trade files. A third program, AOL Parental Controls, allows parents to block access to file-sharing programs, but only when the user accesses the Internet connection through AOL.[10] *See* Table 2.

Table 2

Ability of Parental Control Programs to Block Use of File-Sharing Programs

Parental Control Program	Ability to block pornography on P2P networks	Ability to block all file-sharing	Comments
Cyber Sentinel	yes	no	Can filter offensive words from file-sharing results.
McAfee Internet Security	no	yes	Can block all file-sharing programs from accessing Internet connection.
Norton Internet Security	no	yes	Can block all file-sharing programs from accessing Internet connection.
AOL Parental Controls	no	for certain users	Can block all file-sharing programs from accessing Internet connections if user accesses Internet connection through AOL.
Net Nanny	no	partial	Can block specified file-sharing programs from opening.

[10] According to AOL, this can be accomplished by choosing parental controls options for kids only, young teen, or mature teen on an AOL dialup or AOL broadband connection.

Zone Alarm Pro	no	partial	Can block specified file-sharing programs from opening.
Cyber Patrol	no	partial	Can block user-specified programs from opening.
Cybersitter	no	partial	Requires extra configuration to block the most popular file-sharing program.
Cyber Snoop	no	no	Can not block file-sharing programs or their content.

Parental Controls in File-Sharing Programs

Another option available to parents is to activate parental control features within the file-sharing programs themselves. All of the popular file-sharing programs examined in this report offer these features. The options are promoted as ways to:

- Block files tagged with keywords either built into the program or entered by the user.
- Filter out adult content.
- Block all visual content, including photos, movies, and other image files.

Tests of these options found significant limitations, however. Five of the programs — Grokster, iMesh, Kazaa, LimeWire, and Morpheus — have keyword blocking, but this option is of limited usefulness in blocking pornography. This option requires parents to identify and manually enter terms that might be associated with pornography.

Four of the programs — BearShare, Grokster, Kazaa, and LimeWire — also have options to filter inappropriate content. These filters likewise work by blocking access to files based on a list of prohibited keywords. According to the makers of Kazaa:

> "The original lists of keywords used . . . were generated and are updated using research gathered from the Internet and external research. The list of keywords resides in the application . . . . This list is not available to the public; otherwise its efficacy would be compromised."[11]

This approach has its limitations. A comprehensive list of terms that would eliminate pornographic titles has yet to be developed. Moreover, pornographic images and videos can be posted without suspect words in their file data, evading detection by any list of keywords. Nevertheless, these options do help to reduce pornographic content measurably when activated. For example, Kazaa has an "adult content" filter which, in Committee staff testing, reduced the number of pornographic files retrieved during searches for "Britney," "Olsen twins," and "Pokemon" to less than 15%.

Another approach offered by some of the programs is to block certain kinds of files. For example, four of the programs — BearShare, Grokster, iMesh, and Kazaa — offer the option to block all visual content, including images and videos. These options successfully block all pornographic visual content by restricting file -sharing to music and text files.

Even these options are not foolproof, however. In the case of Grokster, LimeWire, and Morpheus, there is no password protection. Thus, even if parents activate the blocking features, these features can be deselected by their children. In the case of BearShare, iMesh, and Kazaa, the blocking features are password protected, which is a significant improvement. Even so, any filters and passwords established by parents would be erased by the uninstallation of the program and the reinstallation of another free copy of the software, providing a means to circumvent the controls.

Table 3 summarizes these results.

[11] E-mail communications with technical staff at Sharman Networks, makers of Kazaa. Transmitted by Philip Corwin of Butera & Andrews, counsel for Sharman Networks (Feb. 28, 2003).

Table 3

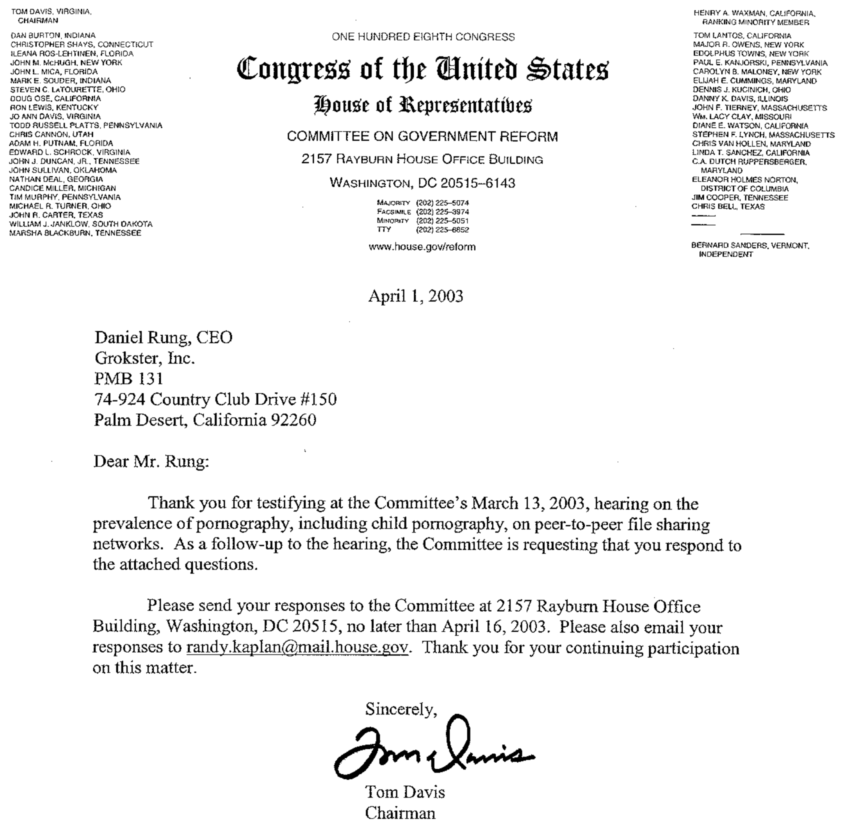
Parental Options within Popular File-Sharing Programs

P2P Application	Has option to block keywords	Has option to filter inappropriate content	Has option to block all visual content	Options can be password-protected	Options remain after reinstallation
Kazaa	●	●	●	●	○
BearShare	○	●	●	●	○
iMesh	●	○	●	●	○
Grokster	●	●	●	○	○
LimeWire	●	●	○	○	○
Morpheus	●	○	○	○	○

● = Yes ○ = No

CONCLUSION

File-sharing programs are popular Internet applications that pose new challenges for parents. In a recent survey, nearly six million pornographic files were available for downloading by children using these programs. Even children who are not searching for pornography are likely to encounter pornographic files when searching for popular entertainers. The parental control programs designed to block children's access to pornography on the Web are generally ineffective when applied to file-sharing programs. A few programs allow parents to block all access to file-sharing programs. Parental control settings found within file-sharing programs can reduce inadvertent exposure to pornography, but these can be circumvented.



TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY	(202) 225–5074
FACSIMILE	(202) 225–3974
MINORITY	(202) 225–5051
TTY	(202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
Wm. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT

April 1, 2003

Daniel Rung, CEO
Grokster, Inc.
PMB 131
74-924 Country Club Drive #150
Palm Desert, California 92260

Dear Mr. Rung:

Thank you for testifying at the Committee's March 13, 2003, hearing on the prevalence of pornography, including child pornography, on peer-to-peer file sharing networks. As a follow-up to the hearing, the Committee is requesting that you respond to the attached questions.

Please send your responses to the Committee at 2157 Rayburn House Office Building, Washington, DC 20515, no later than April 16, 2003. Please also email your responses to randy.kaplan@mail.house.gov. Thank you for your continuing participation on this matter.

Sincerely,

Tom Davis

Tom Davis
Chairman

Questions for the Record – Daniel Rung, CEO, Grokster, Inc.

1. How does file sharing work?

2. Please describe Grokster's business model.

3. What is your company's total annual revenue?

4. What percentage of Grokster's annual revenue is derived from advertising?

5. Please respond to the following question posed by Congressman Christopher Shays (CT) at the hearing:

   How much of Grokster's income is derived from pornography, including child pornography, that is shared on the Grokster network?

6. What are Grokster's other sources of revenues?

7. To what extent does Grokster collect and sell personal information, including email addresses, obtained from its users?

8. What commercial benefit is there for users of peer-to-peer file sharing networks? For example, do users make files available on the network (1) to sell products offered in the file; (2) to provide direct links to other sites where products are available for sale; or (3) to advertise goods or services?

9. Can a person identify the source or other personal information related to a file obtained through sharing files on peer-to-peer networks?

PO Box 642
Charlestown, Nevis
West Indies

Grokster, Ltd.

May 8, 2003

Tom Davis
Chairman
Committee on Government Reform
House of Representatives
Congress of the United States
2157 Rayburn House Office Building
Washington, DC 20515

Mr. Chairman:

Thank you for having allowed me to give testimony at the Hearing on March 13, 2003 regarding pornography as it relates to peer-to-peer networks. At that hearing I was asked to provide additional testimony. I had asked for clarification of the question, which you have provided in your letter dated April 1, 2003 to me. Thank you. In response to the Committee's questions, I provide the following response:

Peer-to-peer file sharing software allows computers connected to a network (such as the Internet) to independently seek each other out and provide connections for the purpose of sharing files of any type. There are several sets of this type of software available including ones using the Gnutella and FastTrack protocols to connect. Grokster is software that allows its users to connect to other user's computers using the FastTrack protocol.

The Grokster software is given to users in exchange for their agreement to accept advertising delivered to their computer. These advertising revenues provide sufficient gross income to pay all of Grokster's expenses, but little net profit. All of Grokster's revenue is derived from advertising. It has no other sources of revenue. Grokster has no ability to collect any personal information about its users while they are using the software.

Grokster derives no revenue from any files, pornographic or otherwise, that are shared between its users. The advertising goes out at the same frequency to the Grokster software any time it is running, no matter what the user is doing or not doing with the software. When the Grokster software is running it could be sitting idle, searching, uploading, downloading, playing files or organizing files among many other activities. The Grokster software can also perform many of these tasks at the same time. Grokster has no direct information about what any of its users are sharing, or whether it is pornographic in nature or not. Accordingly there is no tie between the advertising and whether or not files are being shared.

There are many commercial and non-commercial legitimate uses for peer-to-peer file sharing networks. These include:

- Tens of thousands of musicians distributing their work
- Videos distributed by companies such as JivePlayer
- Distribution of software

- Distribution of video games
- Distribution of eBooks

Generally these users benefit by the distribution of their files to users around the world. Some are happy to just share their files without monetary gain, while others monetize the files via selling the files, selling upgrades to the file, having the file open a website that sells product or "branding" a particular name/product. Since peer-to-peer technology is in its infancy, there will be many new and un-thought-of uses for it in the future.

There is nothing inherent in the Grokster software with which to trace or mark a file in any way. Once a file has gone through the Grokster software, it has neither increased nor decreased its traceability, as the Grokster software has not modified the file in any way. The file itself may have some type of identifying characteristic, such as a "watermark" which could perhaps be used to trace it to its source.

When an actual transfer is taking place, the computer requesting it and the one sending it must know each other's IP address to complete the transfer. During the actual process of transferring a file using most common peer-to-peer software it is possible to obtain the source's IP address using third party tools such as the Netstat command.

Mr. Chairman, thank you for the opportunity to respond to the Committee's questions.

Sincerely,

Daniel Rung
CEO