# ONLINE PORNOGRAPHY: CLOSING THE DOOR ON PERVASIVE SMUT

## HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MAY 6, 2004

**Serial No. 108–90**

Printed for the use of the Committee on Energy and Commerce

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

U.S. GOVERNMENT PRINTING OFFICE

93–980PDF WASHINGTON : 2004

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 ENERGY AND COMMERCE

JOE BARTON, Texas, Chairman

W.J. "BILLY" TAUZIN, Louisiana
RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi, *Vice Chairman*
VITO FOSSELLA, New York
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho
JOHN SULLIVAN, Oklahoma

JOHN D. DINGELL, Michigan
*Ranking Member*
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
TOM ALLEN, Maine
JIM DAVIS, Florida
JANICE D. SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas

BUD ALBRIGHT, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

---

## SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
*Vice Chairman*
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho
JOHN SULLIVAN, Oklahoma
JOE BARTON, Texas,
(Ex Officio)

JANICE D. SCHAKOWSKY, Illinois
*Ranking Member*
CHARLES A. GONZALEZ, Texas
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
BART STUPAK, Michigan
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JIM DAVIS, Florida
JOHN D. DINGELL, Michigan,
(Ex Officio)

# CONTENTS

# ONLINE PORNOGRAPHY: CLOSING THE DOOR ON PERVASIVE SMUT

**THURSDAY, MAY 6, 2004**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10 a.m., in room 2322, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Whitfield, Shimkus, Shadegg, Bass, Pitts, Terry, Ferguson, Issa, Otter, Sullivan, Barton (ex officio), Schakowsky, McCarthy, and Strickland.

Also present: Representative John.

Staff present: Chris Leahy, majority counsel; David Cavicke, majority counsel, Shannon Jacquot, majority counsel; Brian McCullough, majority professional staff; Will Carty, lecislative Clerk; Gregg Rothschild, minority counsel; and Ashley Groesbeck, staff assistant.

Mr. STEARNS. Good morning, everybody. I think we'll start our hearing.

I'm pleased to welcome all of you to the committee, the Subcommittee on Commerce, Trade, and Consumer Protection hearing on online pornography. My colleagues online pornography, both legal and illegal, is a growing problem for legitimate Internet users and in particular, for the most vulnerable among our nation, the children. The explosion growth of online pornography material including the most revolting child pornography continues to be a major issue for all of us.

According to a 2003 report done by the General Accounting Office, there were over 400,000 commercial pornography websites at that time. A subsequent private survey estimated that the number of commercial pornography websites grew from 88,000 in 2000 to 1.6 million today. Now this rapid growth of online pornography on the web becomes even more disturbing when we learn that outright deception and fraud are frequently the means used to dupe legitimate Internet users into exposure, especially when those users are children.

Web pornographers are increasingly using online deception and trickery to lure visitors to their websites. Domain names are being manipulated to appear benign and mousetrap their victims. Spam and fraudulent advertising are being employed to lure unsuspecting visitors, and many of them are children, to obscene

material. And now distributed computing technology like file sharing software applications known as peer-to-peer or P2P software are quickly becoming a favorite medium, particularly to lure our children from the perceived, safety of the family living room out into the dangers of this Internet wilderness.

Especially popular with the most tech savvy, our kids, P2P networks are similar in concept to web browsers, but rather than enabling users to communicate and share information through a central server or website, P2P allows network users access to each others' computers hard drives to share files. While this is an ingenious and a legitimate technology, the chilling fact is that pornographers are now using these P2P applications to target children and young adults with pornographic materials by distributing files with deceptive names that disguise a pornographic file, by labeling it with an entity popular with children or young adults such as an example would be Cinderella or Britney Spears.

According to the Center for Missing and Exploited Children, who will be testifying before us today, from 2001 to 2002 there was a fourfold increase in pornographic material being distributed through P2P networks. This finding, coupled with the fact that many P2P users are children and young adults, makes the risk of inadvertent exposure of pornographic material to children a very significant issue.

As several of our witnesses today will explain, it is very important to recognize that distributed computing technology that enables P2P software is legitimate and frankly a neutral technology with tremendous potential to do good. But it also spawned exciting new applications and it also spawns exciting new applications for legitimate activity. For example, it can enable the establishment of online communities, complete online communities, enhance grid computing and in short, make the market of ideas and information more accessible and obviously more affordable to all Americans.

The power of P2P networks has already led to some outstanding success in the sciences and in mathematics. I'd like to commend my colleague, Mr. Pitts from Pennsylvania, for his leadership in helping cast some light on the very real problems of P2P technology and what it poses, including the ways in which it can facilitate the illegal and disgusting behavior of those that prey upon our children.

I would also like to especially welcome Mr. Norb Dunkel and Mr. Rob Bird who were kind enough to travel from the University of Florida to testify before us today. I am honored to represent the University of Florida, an institution that is innovative on many levels. And particularly, the University of Florida has taken a novel approach to dealing with this misuse of peer-to-peer technology by instituting a system called Integrated Computer Application for Recognizing User Services or ICARUS. ICARUS has successfully harnessed technology to restrict illegal file sharing while preserving P2P for legitimate academic and social activity over the University of Florida's network.

And finally, my colleagues, I look forward to further exploring ways we can ensure the doors to the Internet wilderness remain locked for the sake of our children, unless extreme care is exercised and proper safeguards are in place.

There is clearly no open door policy in cyberspace. As we have seen open doors can also allow infestation by malicious computer viruses, secret spyware downloads, as we learned last week, and now the distribution of online pornography, particularly child pornography.

And as we will learn from the Federal Bureau of Investigation and the Federal Trade Commission, apart from our parental responsibility to carefully supervise our children's Internet activities, there's also need for vigilant and aggressive enforcement measures and prosecution for those who seek to victimize and exploit our children.

I welcome the witnesses today and I look forward to the testimony.

With that, I'm very pleased to recognize Ranking Member Schakowsky.

Ms. SCHAKOWSKY. Thank you, Chairman Stearns, for holding this hearing on children being able to access pornography on the Internet by using peer-to-peer or P2P networking. I'm particularly glad this morning to see that there are a number of young people. I want to point out there are some empty seats for people to sit down, so if you ever wonder whether or not anything we do here in this capital directly affects your lives, this is a good example of one of them that does.

Like you, Mr. Chairman, I'm very concerned about protecting children from the violation and abuse of child pornography and when the Child Sex Crimes Wiretapping Act and the Child Obscenity and Pornography Prevention Act were on the House floor in the last Congress, I voted for them. I believe that these bills would go a long way to safeguard our children from pornography. And I'm also concerned about children's exposure to pornography, in general. I believe that parents should be able to guard against their children stumbling across it on the Internet, but in ways that do not violate the first amendment.

As the testimony demonstrates, the user of P2P traffic and child pornography continues to grow. And it is certainly appropriate for the subcommittee to investigate and address this problem. However, peer-to-peer networking is not the main source for child pornography. As the National Center for Missing and Exploited Children CyberTipline found in 2003, there were 840 reports of P2P being the source of child pornography out of 62,369 tips received; websites with the source of 45,035 of the reports.

Since 1998, P2P has been the source for only 1 percent of online child pornography. P2P systems and the distributed competing technologies behind it do not much more than serve as—do much more than serve as access to pornography. Some uses are interesting and innovative like using it for environmental and biomedical research as Dr. Catlett from the University of Chicago and Argonne Lab explains in his testimony. Other uses are seriously distressing like the unauthorized downloading of copyrighted materials and the spreading of spyware and viruses. When discussing P2P, we cannot ignore these uses. I'm glad that we have a number of witnesses here today who will go over these points as well.

P2P is a lot like other issues we've had to deal with in our subcommittee as with the data base bill and spyware, we have to find

ways to balance concerns. With P2P, we must make sure that artists are compensated for their work and that copyrights are not infringed upon. At the same time we should examine the possibility of P2P as a legitimate way for artists to distribute and market their work when they cannot get play on the stations owned by mega conglomerates.

We also have to look at how to protect our children without making the regulations of a potentially useful technology so onerous that we could lose an innovative system. Although I don't know, I don't have a suggestion at the moment where this balance will fall, I'm very glad that we're here today beginning a discussion on how best to approach the problems that inevitably surface with evolving technologies.

Thank you.

Mr. STEARNS. I thank the gentlelady and we have the chairman of the Energy and Commerce Committee, Mr. Barton, the gentleman from Texas.

Chairman BARTON. Thank you, Mr. Stearns, and thank you for hosting this hearing. I want to commend you and Congressman Pitts for your efforts in this area. It's an important and timely topic as new technologies offer quicker and easier channels for distributing pornographic images over the Internet. Those involved in delivering pornography through deceptive means have used many mechanisms to facilitate their scams. This committee, along with the Committee on the Judiciary has worked very hard to prevent the viewing of pornographic content by unwitting e-mail users by developing brown paper wrapper provisions in the CAN-SPAM Act. I understand those provisions are going to be taking effect later this summer. I expect that enforcement will receive significant attention by both the FTC and the FBI.

What is less well known is the use of peer-to-peer networks in distributing pornography. Children, as large numbers of users of peer-to-peer networks are at significant risk of inadvertent exposure to pornographic images. Some of the pornographic content is disguised as files that look like popular files that children might access. The GAO has reported that searches on key words that might be used by children or young adults have produced a high number of pornographic images, specifically searches retrieved 56 percent pornography. Less than half produced legitimate content sought by children and most disturbing of all, a small, but not insignificant percentage even contained child pornography.

These results highlight three issues that are significant regarding pornography over peer-to-peer networks. Before I close, I want to comment that I believe that the pornography problem over the peer-to-peer network is a problem of illegal behavior related to content, not necessarily the technology itself. Distributed computing is more than just peer-to-peer file sharing of music and other pop culture type files. It's an exciting area with scientific benefits and medical benefits that will accrue to our country's benefit for many years to come.

I look forward to hearing about the other positive uses of distributed computing and hope that this committee can weigh the benefits of distributed computing as we look at ways to solve the peer-to-peer sharing of pornographic files to children.

I again want to thank Congressman Pitts for his attention to this issue and I want to commend Chairman Stearns for your willingness to hold a hearing on this important issue and I yield back the balance of my time.

Mr. STEARNS. I thank the chairman and now the author of a bill dealing with this subject from which we're having the hearing, Mr. Pitts is recognized.

Mr. PITTS. Thank you, Mr. Chairman, for convening this important hearing on the dangers to our children from peer-to-peer file sharing software. Before I start, I'd like to insert into the record a letter.

Mr. STEARNS. By unanimous consent, so ordered.

[The letter follows:]

UNITED STATES SENATE
WASHINGTON, DC 20510
*May 4, 2004*

The Honorable TIMOTHY J. MURIS, *Chairman*
The Honorable MOZELLE W. THOMPSON, *Commissioner*
The Honorable ORSON SWINDLE, *Commissioner*
The Honorable THOMAS B. LEARY, *Commissioner*
The Honorable PAMELA JONES HARBOUR, *Commissioner*
*Federal Trade Commission*
*600 Pennsylvania Avenue, N.W.*
*Washington, DC 20580*

DEAR MR. CHAIRMAN AND COMMISSIONERS:

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

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

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

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

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

Unsurprisingly, these dark alleys tend to become havens for piracy, pornography and computer viruses.

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

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

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

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

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

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

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

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

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

Testimony and news reports show that some users of file-sharing software—particularly children—do not yet realize that downloading popular music or movies "for free" is usually unlawful. Many users may not realize that downloading or redistributing infringing works can be a federal crime, and may not know the severity of the penalties for copyright infringement. These users cannot be adequately educated by vague warnings to "obey the law": Review of the Copyright Act will not disclose which files may be illegal to download, the prevalence of infringing works on a network, or the risks of letting a clever designer limit his own risks of liability by using your home computer to house network search indices much like those that exposed the original Napster to staggering secondary liability for infringement.

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

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

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

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

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

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

ecute any enforcement actions justified by any potential violations of the Act disclosed.

Sincerely,

PATRICK LEAHY
*United States Senator*
ORRIN G. HATCH
*United States Senator*
BARBARA BOXER
*United States Senator*
TED STEVENS
*United States Senator*
GORDON SMITH
*United States Senator*

Mr. PITTS. Thank you. There are millions of people using peer-to-peer software at any given time. Approximately 40 percent of the users are children. Our children download peer-to-peer software in hopes that they can get their hands on free music or movies, but I'm not here to talk about copyrights or what artists or musicians are entitled to. That's an important and necessary discussion to have. But I'm afraid it has become a smokescreen for a very real danger facing our children in the use of peer-to-peer software. Kids log on to Kazaa or LimeWire looking music. Instead, when they search for songs by their favorite music group or pictures of their favorite baseball player, they get porn, a lot of it illegal child pornography.

A search for files relating to children's characters such as Elmo or Snow White, therefore yields an alarming amount of pornography. One has to ask why are these files misnamed? An adult looking for pornography isn't going to search for Elmo. Maybe he would if he's a pedophile and it's code talk for illegal material. Perhaps our friends at Kazaa would like to let us know if that is happening. Children are the only possible target of this false labeling.

I have a printout here, some printouts and they represent the results of searches done on Kazaa on these topics and the results are shocking. These searches were done using the adult filter that Kazaa offers. If members want to see it for themselves, I'll let you see this. If a child accidentally downloads a file containing child pornography, the pedophile distributing it has instant access to the child. He can easily communicate with the child over the Internet, drawing the child into his web. And that's exactly what they want. Pedophiles often lure children into viewing pornography to encourage their victims to engage in sex. This is the way pedophiles operate in the real and cyber world.

As evidence of this trend, Suffolk County, New York last year arrested 12 individuals in a sting operation. They used Kazaa to distribute their child pornography. The confiscated files that were distributed showed children being raped. One had an audio with a child screaming "stop, Daddy, stop."

Now some proponents of peer-to-peer say that in proportion to the Internet at large the amount of pornography on peer-to-peer networks is meager. I agree that pornography is rampant on the Internet, but this finger pointing is a pretty bad way to pass the buck. If you go to the most popular search engine, Google, and type in the same words, you don't get child porn. You get what you ask for. You type in Cinderella or Pokeyman, Snow White, baseball,

you get information on Cinderella, Pokeyman, Snow White and baseball.

Even if pornography comes up in these searches, it's far down the list. And parents can rely on filters to block much of that material from ever appearing on a computer screen. This is not the case with peer-to-peer software. If you enter these terms in your peer-to-peer search window, the results are primarily pornographic material. Any time you have millions of children having easy access to such horrible material, I don't care if you claim someone else has more, if your product facilitates or encourages illegal activity, if your product allows predators, pornographers, pedophiles to prey on children and leads to the abuse of just one child, while you stand idly by, you have no excuse.

This is not about the recording industry. It's about the peer-to-peer industry. Peer-to-peer distributors should be held accountable for the smut that they actively put into the hands of our children. They should be expected to allow parents to protect their children, not ridicule their efforts to do so.

Now we'll hear today about peer-to-peer software's filters and parents' passwords. They don't work. They do not protect children from receiving pornography. This is because they are key word filters that only prevent children from searching for pornography. Just look at these printouts, these searches are proof. They were done with the adult filter on and the results are shocking because pornographers rename their files to sound innocent. The filters are ineffective.

Further, parents think that they have existing Internet filters that protect their children, but they don't work on peer-to-peer software either. Netnanny doesn't work. CyberPatrol doesn't work. And peer-to-peer filters don't work. In fact, not only are they ineffective, they're easy to circumvent. Any 13-year-old can turn them off. We need to protect the millions of children using peer-to-peer software and that is why last year my colleague, Chris John, and I introduced H.R. 2885, Protecting Children from Peer-to-Peer Pornography Act. This bill raises awareness of the dangers of peer-to-peer software. It calls on the FTC to hold peer-to-peer distributors accountable for the smut that they actively put into the hands of our children and peer-to-peer networks may not want to stop this because it means less users or less material or less revenue.

Our bill would empower parents by giving them the tools they need to cutoff the flow of harmful information into their homes and it would aid the development of technology to block peer-to-peer installation. This is a threat that harms our kids. It's time to do something about it.

Again, thank you, Mr. Chairman, for the hearing. I look forward to hearing the testimony of the witnesses.

Mr. STEARNS. I thank my colleague and if you don't mind I think you could circulate that to the members so that they have an opportunity to see it. And the gentleman from Nebraska, Mr. Terry.

Mr. TERRY. Thank you, Mr. Chairman, I'm anxious to hear from our witnesses today. This is an important issue and I'll just give you a story. Over the weekend, last week my son who is 9 years old is becoming darn proficient in exploration of the Internet with my supervision, said that he wanted to download some music. He

wanted some Aerosmith songs. That in and of itself made me rather proud of him. Not Britney Spears, Aerosmith, that's my boy. So I said all right, let's go on and we're going to do this right. And so went to Real Music. We paid for the four Aerosmith songs that I knew didn't have sexually explicit language in them which even Aerosmith makes some sexual references in their songs so we had a few, Sweet Emotion, Dream On, not Love in an Elevator. But we did it the right way. I wanted to make sure he did it the right way by paying for this music. By the way, for the four songs he had to sweep the patio and earn it. But the value of that these artists and record companies have invested and their rights to this music should be protected.

But also, I wanted to make sure that he wasn't on other sites like Kazaa because even at 9 years of age his friends know what Kazaa is and have gone on Kazaa. And when I see what Mr. Pitts, my colleague from Pennsylvania has introduced here, about how easy it would be for a 9-year-old boy to access hard core pornography, in trying to do something as simple as download a song for free.

When I talk to high school classes, and just like the ranking member from Chicago mentioned, that we have a lot of youth here and this is one of the areas that we show Congress actually can effect, I ask high school students when I speak to their class, how many of them download music? Inevitably about 80 percent of the class, no matter where I am in Omaha or my District, 80 percent of the class will raise their hand. Then I ask for those raising their hands, how many have paid for that music? Probably two or three hands out of that entire class will remain up which means this is what our high school students are seeing on a daily basis.

And most of them are probably savvy enough to choose the music versus the some rather explicit nature of the title here for the pornography. But what also concerns me is not only the volume of what our students are being exposed to, but also just in the very fact that they disguise this and you don't have a way like on some of the legitimate music, when you buy it, you can click on it and they'll give you a 30 second demo so you know what you're buying before you click on it. Here, you have to click on it and download it before you know. So if they've disguised it as a Britney Spears song, you don't know that until you open up the file after it's been downloaded. Those are some of the dangers that we're here to explore.

So I appreciate, Mr. Chairman, you holding this because this is an important protection of our children in the cyber age.

Mr. STEARNS. I thank my colleague. The gentleman from New Jersey, Mr. Ferguson.

Mr. FERGUSON. Thank you, Mr. Chairman. Thanks for holding this hearing on a matter that's of great concern to families like mine and families as we've heard across this country. The scourge of online pornography has allowed sexual predators bent on luring our children into their perverse world to enter our homes through our computers and the open doors of an Internet connection.

A March 2003 GAO study found over 400,000 commercial pornography sites on the Internet and more recent estimates have found that the number is increasing exponentially. But even more dis-

turbing than the sheer volume of Internet pornography outlets are the increasingly bold and pervasive practices by sexual predators who attempt to lure children onto their dangerous websites and we've heard some examples of that already this morning.

As a father of three young kids, we have our fourth due this summer. I'm concerned. Our kids don't use the Internet yet, but they will. They'll have to if they're to operate in our world today. I'm concerned about our children's ability to use the Internet without being targeted by people who have malicious intent. I mean I have AOL. Anybody who has AOL knows that you get e-mails, unsolicited e-mails, you get spam e-mails every day with unbelievable titles and subjects and trying to lure you to these various sites.

I really look forward to hearing from our witnesses today about what's currently being done, but really more importantly about what can be done, what needs to be done in the future and what we can do to protect our children from this kind of menace.

I want to thank you again, Mr. Chairman, for holding this hearing. I know we have some very distinguished panelists here today, some of whom we know and we appreciate their work outside of this committee room, but certainly appreciate them being here today to share some of their experiences with us and what we can be doing in the Congress to protect our children across this country.

Thanks again, Mr. Chairman, I yield back.

Mr. STEARNS. I thank my colleagues. The gentleman from New Hampshire, Mr. Bass.

Mr. BASS. No opening statement.

Mr. STEARNS. No opening statement. The gentleman from Idaho, Mr. Otter.

Mr. OTTER. I will submit my statement.

Mr. STEARNS. By unanimous consent, so ordered.

[Additional statement submitted for the record follow:]

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Thank you, Mr. Chairman, for holding this timely hearing. Over the past several weeks, this subcommittee has delved into several concerning issues indirectly related to the constantly developing technology available on the Internet. Today's hearing will provide us with an excellent opportunity to examine what steps have been and should be taken to limit the availability of pornographic material via the Internet.

I would also like to thank the distinguished panelists who have joined us today. The ladies and gentlemen who have agreed to appear today are top experts in their fields. I look forward to their testimony and first-hand insight to help this subcommittee shape a better understanding of what role Congress may be able to play in eliminating the spread of pornography via peer-to-peer file sharing programs.

In the preceding weeks, this subcommittee has acquired an in-depth understanding of the invasive and intrusive ways our families and businesses can be affected by the Internet. The deceptive and misleading tactics pornographic websites employ to attract unwitting visitors to their sites cannot be tolerated, particularly when they seek to victimize children. Congress has acted to make the pornographic exploitation of children illegal, but the ever-increasing technology of the Internet makes the enforcement of these laws exceptionally difficult.

I look forward today to uncovering what steps are being taken to regulate the dispersal of pornography via peer-to-peer applications. Similar to the issues this subcommittee has addressed in previous weeks, we must find a way to balance the valid, useful functions of peer-to-peer networking with the need to regulate the illegal and inappropriate uses of this technological infrastructure. I am certain that the

experts joining us today will impart valuable insight on how Congress may be able to properly legislate in an effort to better protect America's youth.

Thank you chairman and I yield back the balance of my time.

---

PREPARED STATEMENT OF HON. JOHN SULLIVAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OKLAHOMA

Thank you Chairman for holding this hearing. This is a *most* important topic.

Pedophiles and Internet obscenity addicts are swapping thousands of hardcore images of sexual abuse of women and children in a new form of computer obscenity that police believe is feeding a demand for more real-time victims of abuse.

*Children are abused.* Millions of children worldwide are abused sexually, and then exploited further by having images and videos of the abuse sold online. This is abuse of the most detestable kind. Both obscenity and child pornography are illegal, and should be prosecuted to the fullest extent of the law.

*Women are exploited.* Worldwide, women are trafficked across borders for use in this material. They are brought to the U.S. and other countries to be used in prostitution and for online obscenity, with proceeds lining the pockets of criminals and no hope in sight for their release from what is bondage, or modern slavery.

*This is the very definition of evil.*

*Obscenity is illegal under federal law.* Title 18 of the U.S. Code clearly states that obscenity is illegal. Further, the Supreme Court delineated in the landmark *Miller vs. California* ruling that obscenity is both definable and illegal under federal law.

But resources available to police to tackle peer-to-peer obscenity and child porn are limited and though they are catching some offenders, it may take months or even years to track down the location of some victims. In such cases, officers monitoring the images can only watch as the women and children grow older and continue to be abused.

*Americans continue to believe that the Federal laws against Internet obscenity should be vigorously enforced,* according to results of a recent poll conducted by Wirthlin Worldwide for Morality in Media. **72%** of Americans from all political perspectives strongly agreed that obscenity laws should be vigorously enforced.

I have introduced H. Con. Res 298, a resolution stating the sense of the Congress that federal obscenity laws should be vigorously enforced throughout the United States. It is important that the House go on the record against this hideous abuse, as the Senate has already done. I will continue to work with my colleagues to see that the abuse of women and children through pornography and obscenity, **ENDS.**

I yield back the balance of my time.

Mr. STEARNS. I think we've finished with our opening statements and we'll go to our first panel of witnesses. We have Mr. Howard Beales, Director, Bureau of Consumer Protection, the U.S. Federal Trade Commission, welcome. We've had you quite a number of times recently. We appreciate your attending. Mr. Keith Lourdeau, Deputy Assistant Director, Federal Bureau of Investigation, Cyber Division, welcome. And Ms. Linda Koontz, Director for Information Management Issues, U.S. General Accounting Office.

And Mr. Beales, we'll start with you with your opening statement. Thank you.

**STATEMENTS OF J. HOWARD BEALES III, DIRECTOR, BUREAU OF CONSUMER PROTECTION, U.S. FEDERAL TRADE COMMISSION; KEITH L. LOURDEAU, DEPUTY ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION; AND LINDA D. KOONTZ, DIRECTOR FOR MANAGEMENT ISSUES, U.S. GENERAL ACCOUNTING OFFICE**

Mr. BEALES. Thank you, Mr. Chairman, it's always a pleasure to be here. And thank you for providing the FTC with this opportunity to submit testimony. My written testimony represents the views of the Federal Trade Commission and my comments orally do not necessarily reflect the views of the Commission or any individual Commissioner.

I'm here today to discuss the Commission's law enforcement efforts combatting Internet fraud and to discuss examples of Internet fraud cases where the fraud involves tricking consumers into viewing online pornography. Although the Internet has empowered consumers with instant access to a breadth of information about products and services that would have been unimaginable 20 years ago, fraud artists have proven adept at exploiting this new technology for their own gain. They are the ultimate early adopters of new technology and they've seized on the Internet as a ready vehicle to find victims for their scams.

To combat these new frauds, the FTC has brought over 300 Internet-related enforcement actions. A number of these actions were against alleged purveyors of online pornography. For example, the Commission sued John Zuccarini who registered some 6,000 domain names that were misspellings of popular websites for mousetrapping consumers. In a ploy designed to capture teenaged and younger Internet users, Zuccarini registered, for example, 15 variations of the popular children's cartoonsite, cartoon network.com. For example, if you typed in cartoon netwok instead of network, you ended at one of his sites. He also registered 41 variations in the name of teen pop star Britney Spears. Surfers who looked for a site, but misspelled the web address were taken to Zuccarini's sites. Once there, he took control of their Internet browsers and forced the consumers to views explicit advertisements for pornographic websites, as well as websites advertising gambling and psychic services. The obstruction was so severe in this case that consumers were often forced to choose between taking up the 20 minutes to close all the windows that opened or restarting their computer and losing their pre-mousetrap work.

Mr. Zuccarini faced both our civil lawsuit as well as criminal prosecution by the U.S. Attorney for the Southern District of New York. The U.S. Attorney charged Zuccarini with violations of the Truth in Domain Names Act which is part of the Amber Alert law Congress enacted last spring. Mr. Zuccarini pled guilty to 49 counts of violating the act and the one count concerning the possession of child pornography. In February 2004, the Court sentenced Mr. Zuccarini to 30 months in prison. In addition, the Commission obtained a permanent injunction barring Zuccarini from engaging in mousetrapping and imposing a $1.8 million judgment.

Similarly, unsolicited commercial e-mail, or spam, is a nuisance, but is also a ready source of fraud, including fraudulent methods that expose children to pornography. In a recent case against a spammer, the Commission alleged that the defendant sent e-mail messages claiming that the consumer had won a free Sony PlayStation 2 or other prize through a promotion that was purportedly sponsored by Yahoo. It was another ploy that was particularly attractive to children. Instead, in five mouse clicks you ended up on a pornographic website connected to a 900 number and being charged $4 a minute. The Commission obtained a Court order to end this practice.

As the name of the CAN-SPAM Act implies addressing the abuses inflicted on the American public by purveyors of pornography was one of Congress' primary purposes in passing the legislation.

The Act directed the FTC to adopt a rule requiring a mark or notice to be included in spam containing sexually oriented material. The purpose of the notice is to inform recipients and to make it easier to filter out messages that recipients do not wish to receive.

Our final rule requires that the phrase "sexually explicit:" to be included in spam that includes either visual images or written descriptions of sexually explicit conduct. The rule requires this phrase both in the subject line and in the electronic equivalent of a brown paper wrapper in the body of the message. This brown paper wrapper must be viewed before the user if it encounters any other information or images.

The rule's effective date is May 19 of this year, so starting then failure to include the warning will result in fines for violating the FTC AcT or Federal criminal prosecution.

As documented by reports from the General Accounting Office and the House Committee on Government Reform, another source of pornographic content online is peer-to-peer file sharing software. P2P file sharing software enables users to exchange files with other users. The FTC has engaged in educational efforts to assist consumers in protecting themselves from the risk of harm when they're downloading and using this technology.

To warn consumers, and particularly parents, about the risk that P2P software can pose, in July 2003, the FTC issued a consumer alert. In this alert, the Commission warned consumers that file sharing software may be used to exchange pornography as well as games, videos and music that may be inappropriate for children. The FTC also alerted consumers to the security risks of improperly configuring P2P file sharing software including the risk that sensitive personal files inadvertently may be disclosed.

We will continue to take action against fraud artists who use technology to trap consumers into viewing sexually explicit content. In just a few weeks, the CAN-SPAM rulemaking requiring clear notice to consumers will take effect and those who use e-mail to send such content had better take notice themselves.

Thank you, and I look forward to answering any questions.

[The prepared statement of J. Howard Beales III follows:]

PREPARED STATEMENT OF HOWARD BEALES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. Chairman and members of the Committee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission ("Commission" or "FTC").[1] I appreciate this opportunity to provide the Commission's views on peer-to-peer file-sharing and protecting consumers online. This testimony, among other things, addresses the Commission's law enforcement actions against fraud artists whose deceptive or unfair practices involve exposing consumers, including children,[2] to unwanted pornography on the Internet.[3] The testimony also recognizes that some peer-to-peer file sharing services, as opposed to other content providers that operate their own networks, may not provide sufficient opportunities for labeling or other

[1] The written statement presents the views of the Federal Trade Commission. Oral statements and responses to questions reflect my views and not necessarily those of the Commission or any individual Commissioner.

[2] As the Committee is aware, the Commission also enforces the Children's Online Privacy Protection Rule, which requires Web sites, primarily those directed to children, to obtain parental consent before collecting personal information from children under the age of 13. Our enforcement and education efforts under this Rule are not addressed in the testimony.

[3] The Commission has brought cases involving unfair or deceptive acts or practices related to the dissemination of online pornography to adults. *See, e.g., FTC v. Brian D. Westby* (FTC File No. 032 3030; Case No. 03 C 2540; ND IL; filed Apr. 15, 2003; released Apr. 17, 2003).

controls that parents may find useful in protecting their children from objectionable content.

The Federal Trade Commission is the federal government's principal consumer protection agency. Congress has directed the Commission, under the FTC Act, to take law enforcement action against "unfair or deceptive acts or practices" in almost all sectors of the economy and to promote vigorous competition in the marketplace.[4] With the exception of certain industries and activities, the FTC Act provides the Commission with broad investigative and enforcement authority over entities engaged in, or whose business affects, commerce.[5] The FTC Act also authorizes the Commission to conduct studies and collect information, and, in the public interest, to publish reports on the information it obtains.[6]

Although the Internet has empowered consumers with instant access to a breadth of information about products and services that would have been unimaginable 20 years ago, fraud artists also have proven adept at exploiting this new technology for their own gain. They are the ultimate "early adopters" of new technology. And, they have seized on the Internet as a ready vehicle to find victims for their scams. In fact, the Commission's consumer complaint data show that consumers increasingly report the Internet as the initial point of contact for fraud, and that the Internet has now outstripped the telephone as the source of first contact for fraud.

Many of these frauds are simply online variations of familiar, offline scams. To combat these new frauds, the FTC has brought over 300 Internet-related enforcement actions, including actions against alleged purveyors of online pornography. For example, the Commission sued John Zuccarini, who registered some 6,000 domain names that were misspellings of popular Web sites, for "mousetrapping" consumers.[7] In a ploy designed to capture teenaged and younger Internet users, Zuccarini registered 15 variations of the popular children's cartoon site, www.cartoon network.com, (e.g., "cartoon netwok" instead of "cartoon network") and 41 variations on the name of teen pop star, Britney Spears. The Commission alleged in its complaint that surfers who looked for a site, but misspelled its Web address, were taken to the defendant's sites. Once consumers arrived, Zuccarini's Web sites were programmed to take control of their Internet browsers and force the consumers to view explicit advertisements for pornographic Web sites, as well as Web sites advertising gambling and psychic services. The obstruction allegedly was so severe in this case that consumers often were forced to choose between taking up to twenty minutes to close out all of the Internet windows, or turning off their computers, and losing all of their "pre-mousetrap" work.

After being sued, Mr. Zuccarini disappeared. Fortunately, as a result of a cooperative working relationship between the FTC and the United States Attorney's Office for the Southern District of New York, Mr. Zuccarini was arrested in a south Florida hotel room.[8] The U.S. Attorney's Office issued an indictment charging Zuccarini with violations of the Truth in Domain Names Act.[9] He pled guilty to 49 counts of violating the Act and to one count concerning the possession of child pornography. In February 2004, the court sentenced Mr. Zuccarini to 30 months in prison. In addition, the Commission obtained a permanent injunction barring Zuccarini from engaging in mousetrapping and imposing a $1.8 million judgment.[10]

Similarly, unsolicited commercial email, or spam, is a nuisance, but it is also a ready source of fraud, including the fraudulent means to expose children to pornography. In a recent case against a spammer, the Commission alleged that the defendant sent email messages claiming that consumers had won a free Sony PlayStation 2 or other prize through a promotion purportedly sponsored by Yahoo, Inc., another

---

[4] 15 U.S.C. § 45.

[5] In addition to the FTC Act, the Commission also has responsibility under 46 additional statutes governing specific industries and practices.

[6] 15 U.S.C. § 46(b) and (f). Section 46(f) of the FTC Act provides that "the Commission shall also have the power . . . to make public from time to time such portions of the information obtained by it hereunder as are in the public interest; and to make annual and special reports to Congress . . ."

[7] *FTC v. John Zuccarini,* No. 01-CV-4854 (E.D. Pa. 2002).

[8] Benjamin Weiser, *Spelling It 'Dinsey,' Children on Web Got XXX,* N.Y. TIMES, Sept. 4, 2003, § B (Late Edition), at 1. At the time of his arrest, Mr. Zuccarini was surrounded by computer equipment and cash, all of which was seized by criminal authorities. A United States Postal Inspector served him with the Final Court Order in the Commission's case.

[9] The Truth in Domain Names Act makes it unlawful to knowingly use a misleading domain name with the intent to attract a minor into viewing a visual depiction of sexually explicit conduct on the Internet. *See* 18 U.S.C. § 2252(B)(b). This Act is contained in the new "Amber Alert" law enacted in 2003.

[10] *See* www.ftc.gov/opa/2002/05/cupcake.htm.

ploy particularly attractive to children.[11] The Commission alleged that the Web site link contained in the email instead directed consumers first to a Web page that imitated the authentic Yahoo Web page. The imitation Yahoo Web site instructed consumers to download a program that supposedly would allow them to connect "toll-free" to a Web site where they could enter their name and address to claim their PlayStation 2. Consumers who followed the instructions were connected to a pornographic Web site through a 900-number, where they incurred charges of up to $3.99 per minute. The Commission obtained orders barring the spammers from sending any email that misrepresents the identity of the sender or the subject of the email. The Commission also obtained a settlement with the company that created the modem software used by the spammers in this scheme which includes the requirement that it pay $25,000 in alleged ill-gotten gains.[12]

As the name of the CAN-SPAM Act implies (Controlling the Assault of Non-Solicited Pornography and Marketing Act), addressing the abuses inflicted on the American public by purveyors of pornography was one of Congress' primary purposes in passing that legislation.

Section 5(d) of the CAN-SPAM Act[13] directed the Federal Trade Commission to adopt a rule requiring a mark or notice to be included in spam that contains sexually oriented material. The purpose of the notice is to inform recipients that a spam message contains sexually oriented material and to make it easier to filter out messages that recipients do not wish to receive.

The FTC's final rule prescribes the phrase "SEXUALLY-EXPLICIT:" as the mark or notice mandated by the CAN-SPAM Act[14] to be included in spam that includes either visual images or written descriptions of sexually explicit conduct.[15] The final rule follows the intention of the CAN-SPAM Act to protect email recipients from exposure to unwanted sexual images in spam, by requiring this mark to be included both in the subject line of any email message that contains sexually oriented material and in the electronic equivalent of a "brown paper wrapper" in the body of the message. This "brown paper wrapper" is what a recipient initially will see when opening a message containing sexually oriented material. The "brown paper wrapper" will include the prescribed mark or notice, certain other specified information, and no other information or images.

The Rule's effective date is May 19, 2004, so starting then, senders of spam email that contains sexually oriented material must include the warning "SEXUALLY-EXPLICIT: " in the subject line or face fines for violating the FTC Act or federal criminal law.[16]

As documented by reports from the General Accounting Office and the House Committee on Government Reform,[17] another distribution channel for pornographic content online is Peer-to-Peer (P2P) file-sharing software. P2P file-sharing software enables individual users to exchange files with other users. The FTC has engaged in educational efforts to assist consumers in protecting themselves from the risk of harm when they are downloading and using P2P file-sharing technology.

To warn consumers, including parents, about the risk that P2P software can pose, including the risk of exposure to online pornography, in July 2003, the FTC issued

---

[11] *FTC v. BTV Industries,* No. CV S-03-1306-LRH-RJJ (D. Nev. 2004).

[12] *Id.* The FTC's complaint against the software company, BTV Industries, and its principals, Rik Covell and Adam Lewis, alleges that the defendants violated the FTC's 900-Number Rule by failing to disclose clearly to consumers using their software that they would be connected to the Internet through a 900-number and would incur charges of up to $3.99 per minute. The settlement permanently bars the defendants from failing to disclose the cost of accessing any 900-number pay-per-call service, as well as from misrepresenting that consumers have won a prize, that consumers will be connected to any Web site toll-free, and that any of BTV's products or services are associated with a third party.

[13] 15 U.S.C. § 7704(d).

[14] The Commission published a notice of proposed rulemaking in the Federal Register on January 29, 2004, and accepted comments until February 17, 2004. The Commission received 89 comments, mostly from individual consumers applauding the Commission's proposal and expressing their concern about pornographic email to which they and their children were being subjected. The final rule also excludes sexually oriented materials from the subject line of a sexually explicit email message.

[15] CAN-SPAM defines "sexually explicit conduct" by reference to the Sexual Exploitation and Other Abuse of Children Act ("Abuse of Children Act"), 18 U.S.C. Section 2256, which in turn defines this phrase to mean "actual or simulated—(i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person."

[16] 18 U.S.C. Section 2256. The Department of Justice enforces Section 2256.

[17] *See infra* note 27.

a consumer alert entitled, "File-Sharing: A Fair Share? Maybe Not."[18] In this alert, the Commission warned consumers that P2P file-sharing software may be used to exchange pornography, as well as games, videos, and music that may be inappropriate for children. The FTC also alerted consumers to the security risks of improperly configuring P2P file-sharing software, including the risk that sensitive personal files inadvertently may be disclosed.[19]

The Commission also recently examined other implications of P2P file-sharing software at its workshop entitled "Monitoring Software on Your PC: Spyware, Adware, and Other Software" held on April 19, 2004.[20] This workshop was designed to provide us with information about the nature and extent of the problems related to spyware.[21]

The testimony at the workshop and the public comments received provide us with some insight concerning the relationship between P2P file-sharing technology and the distribution of spyware.[22] Workshop participants generally agreed that spyware often is bundled with free software applications, including P2P file-sharing software. In addition, participants noted that distributors of the free software—including the disseminators of P2P file-sharing applications—may not adequately disclose the bundling of spyware with the free software.

Some have suggested restricting the downloading of P2P file-sharing software applications to combat the distribution of spyware. Participants at the workshop, however, emphasized that P2P file-sharing technology itself is neutral—but some participants argued that software applications may create harms for consumers. Accordingly, participants generally expressed the view that government and industry responses should focus on the spyware software that itself has adverse effects on consumers.

The Commission will continue to review the information from the workshop and related comments. Later this year, the FTC will issue a comprehensive report addressing spyware, including the relationship between P2P file-sharing software and spyware.

The FTC also has studied the effect of P2P file-sharing software in connection with its long-standing oversight of the marketing of violent entertainment to children. Since September 2000, the Commission has monitored the marketing of violent entertainment products to children by the motion picture, music recording, and electronic games industries. The FTC has issued four reports setting forth its findings.[23]

In connection with its ongoing review of these industries, the Commission staff recently examined four popular P2P file-sharing services to assess what online disclosures, if any, were made regarding the content of individual files shared by users of these services.[24] The four services examined offer consumers the ability to download free software that enables them to share files, including music downloads, with other users.[25] The files do not reside in a central location, but rather are stored on the hard drives of the users of the software. None of the P2P file-sharing services themselves label or otherwise provide notice about the content of any file. Instead, each user of a particular P2P file-sharing program places files in a shared folder

---

[18] *See* "File-Sharing: A Fair Share? Maybe Not," at www.ftc.gov/bcp/conline/pubs/alerts/sharealrt.htm.

[19] In April 2004, the Commission likewise alerted businesses to the potential security risks of P2P file-sharing programs. The Council of Better Business Bureaus, with the cooperation of the Commission and the National Cyber Security Alliance, produced and widely distributed a brochure that provides a checklist of recommendations to help large and small businesses improve their computer security, and specifically alerts businesses to the possible risks associated with file-sharing programs.

[20] 69 Fed. Reg. 8538 (Feb. 24, 2004), at www.ftc.gov/os/2004/02/040217spywareworkshopfrn.pdf.

[21] For the purposes of the workshop, the FTC staff tentatively described spyware as "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." 69 Fed. Reg. 8538 (Feb. 24, 2004), at www.ftc.gov/os/2004/02/040217spywareworkshopfrn.pdf.

[22] The FTC received 200 comments about spyware by the time of the workshop, and public comment on this topic will be accepted until May 21, 2004. Public comments are posted on the FTC's Web site at www.ftc.gov/bcp/workshops/spyware/index.htm#comments.

[23] *See, e.g.,* "Marketing Violent Entertainment to Children: A Review of Self-Regulation and Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries" (Sept. 2000). To date, the Commission has issued three follow-up reports—in April and December of 2001, and in June of 2002.

[24] These file-sharing software services reviewed were Kazaa, Morpheus, LimeWire, and Overnet.

[25] Such services may enable users to upload or download copyrighted recordings without first obtaining permission from the copyright holder.

on his or her own hard drive and thus can label or designate the file in any manner he or she chooses. Accordingly, each file, if labeled or otherwise described as having explicit content, would have been labeled by the individual user.

Each of the P2P file-sharing programs offered some type of filter to exclude unwanted content. Kazaa and LimeWire provided filters that blocked access to materials that contained offensive or otherwise adult-content related words in the description of the file. In addition, all four services gave users the ability to create their own filters by manually entering all the words that they wanted blocked from search results. All of these filters, however, operate by only examining language found in the title or descriptor of the file, rather than the content of the file.[26] Moreover, these filters may not be effective when users label files inaccurately, which can result in the transfer of files with pornographic or other unwanted content.[27]

CONCLUSION

The FTC thanks the Subcommittee for this opportunity to describe how the Commission has used its authority under of Section 5 of the FTC Act to attack deceptive and unfair practices in the distribution of online pornography.

Mr. STEARNS. I thank the gentleman. Welcome and your opening statement.

**STATEMENT OF KEITH L. LOURDEAU**

Mr. LOURDEAU. Good morning, Chairman Stearns, and other members of the subcommittee. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI's role in combatting the exploitation of children from the use of peer-to-peer networks.

The FBI's Innocent Images National Initiative is comprised of 2800 undercover operations. These operations involve FBI Agents online in an undercover capacity to seek child predators and individuals responsible for production and dissemination and possession of child pornography. This is accomplished by using a variety of techniques to include purchasing child pornography from commercial websites, creating online personas to chat in predator chat rooms and co-opting predators e-mail accounts. The Innocent Images has grown exponentially between fiscal year 1996 and 2003 with a 2,050 percent increase in cases opened.

Between fiscal year 1996 and 2003, Innocent Images has recorded over 10,510 cases opened. Recently peer-to-peer networks were identified as a growing problem in dissemination of child pornography. A GAO report published in September of 2003 indicated a fourfold increase in reports complaining of child pornography in peer-to-peer networks. In 2001, the FBI received 156 complaints about child pornography in peer-to-peer networks. By 2002, the number of complaints had risen to 757.

This increase may be attributable among other things, the popularity of peer-to-peer networks, as well as the overall increase of child pornography available on the Internet. These programs are free and are easy to install. In May of 2003, Sharman Networks,

[26] For example, music recordings that have been designated with a parental advisory by a recording company would be blocked by the filter only if a word in the title or descriptor of the file happened to be offensive. A recording company may have decided to apply the Parental Advisory Label to a particular recording for any number of reasons other than the presence of offensive words in the title.

[27] *See, e.g.,* "File-Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography," General Accounting Office Report to the Chairman and Ranking Minority Member, Committee on Government Reform, U.S. House of Representatives (Feb. 2003); and "Children's Access to Pornography Through Internet File-Sharing Programs," prepared for Rep. Henry A. Waxman and Rep. Steve Largent by Minority Staff, Special Investigations Division, Committee on Government Reform, U.S. House of Representatives (July 27, 2001).

a developer of a very popular file sharing program reported that their software had been downloaded more than 230 million times. This software and other file sharing programs like it allow users to share files with anyone on the network. This creates an environment of relative anonymity among users. However, this anonymity is also perceived. Users are not truly anonymous. Using peer-to-peer software users' computers connect directly to one another to share files without going through a central server.

Mr. STEARNS. Mr. Lourdeau, just push the microphone a little closer to you. There are some real nuances that you're saying we want to make sure we get. Go ahead, thanks.

Mr. LOURDEAU. Nevertheless, each time a computer accesses the Internet it is associated with an Internet protocol or IP address. Therefore, despite the fact that a peer-to-peer connection is not facilitated by a central server, users can still be identified in real time by the IP addresses associated with their computers. IP addresses are the only way to definitely identify a particular user on a peer-to-peer network. In this environment, users of peer-to-peer often believe they are anonymous. There is some degree of truth in this assertion as peers in the networks are anonymous to each other. That being said, they are not anonymous to law enforcement. Through the use of covert investigative techniques, administrative subpoenas, Agents can determine which individual users possess and distribute child pornography over these networks. Utilizing search warrants, interviews and computer forensic tools, Agents can strengthen their cases and these individuals are eventually indicted and prosecuted.

During the initial phases of several peer-to-peer investigations, Agents have determined peer-to-peer networks are one of many Internet havens for the open distribution of child pornography. Several of the individuals using peer-to-peer networks to distribute child pornography, openly describe content of the material they share as illegal. This further contributes to the feeling of anonymity in these networks and leads users to become even more brazen in their conduct.

To combat this, the FBI has created an investigative protocol for peer-to-peer investigations to begin aggressively apprehending offenders. After developing peer-to-peer investigative protocol, the Department of Justice's Child Exploitation and Obscenity Section, a number of cases were initiated to determine the technique's viability. Detailed discussion of these cases could possibly jeopardize on-going investigations, however, I'd like to assure the subcommittee that the FBI is aggressively pursuing the trade of child pornography on peer-to-peer networks.

In these investigations, Agents have found child pornography to be readily available using most basic of search terms. Often child pornography was easily available when innocuous search terms were used such as Britney Spears, or the word young. The FBI recently started a new initiative with America's Most Wanted where photographs of unidentified subjects involving child pornography are aired on the program. John Doe arrest warrants are obtained and the unknown subjects when located are arrested for their crimes. The FBI has received outstanding support from the public in this initiative.

The FBI, along with our law enforcement and private industry partners, continue to combat the crime problem of child pornography over the Internet. We have and continue to target websites which host child pornography, Internet news groups, file servers and subjects who utilize peer-to-peer file sharing programs who exchange child pornography.

In closing, the FBI looks forward to working with other law enforcement agencies, private industry and the Department of Justice in continuing to combat this major crime problem. The protection of our children requires the combined efforts of all sectors of our society.

I would like to thank Chairman Stearns and the committee for the privilege to be here before you and I'll answer any questions. Thank you.

[The prepared statement of Keith L. Lourdeau follows:]

PREPARED STATEMENT OF KEITH L. LOURDEAU, DEPUTY ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

INNOCENT IMAGES NATIONAL INITIATIVE

The Innocent Images National Initiative (IINI), a component of FBI's Cyber Crimes Program, is an intelligence driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation (CP/CSE) facilitated by an online computer. The IINI provides centralized coordination and analysis of case information that by its very nature is national and international in scope, requiring unprecedented coordination with state, local, and international governments, and among FBI field offices and Legal Attachés.

Today computer telecommunications have become one of the most prevalent techniques used by pedophiles to share illegal photographic images of minors and to lure children into illicit sexual relationships. The Internet has dramatically increased the access of the preferential sex offenders to the population they seek to victimize and provides them greater access to a community of people who validate their sexual preferences.

The mission of the IINI is to reduce the vulnerability of children to acts of sexual exploitation and abuse which are facilitated through the use of computers; to identify and rescue witting and unwitting child victims; to investigate and prosecute sexual predators who use the Internet and other online services to sexually exploit children for personal or financial gain; and to strengthen the capabilities of federal, state, local, and international law enforcement through training programs and investigative assistance.

THE HISTORY OF THE INNOCENT IMAGES NATIONAL INITIATIVE:

While investigating the disappearance of a juvenile in May 1993, FBI Special Agents and Prince George's County, Maryland, Police detectives identified two suspects who had sexually exploited numerous juveniles over a 25-year period. Investigation into these activities determined that adults were routinely utilizing computers to transmit sexually explicit images to minors, and in some instances to lure minors into engaging in illicit sexual activity. Further investigation and discussions with experts, both within the FBI and in the private sector, revealed that the utilization of computer telecommunications was rapidly becoming one of the most prevalent techniques by which some sex offenders shared pornographic images of minors and identified and recruited children into sexually illicit relationships. In 1995, based on information developed during this investigation, the Innocent Images National Initiative was started to address the illicit activities conducted by users of commercial and private online services and the Internet.

The IINI is managed by the Innocent Images Unit within the FBI's Cyber Division at FBI Headquarters in Washington, DC. Innocent Images field supervisors and investigative personnel work closely with the Innocent Images Unit regarding all IINI investigative, administrative, policy, and training matters. The IINI provides a coordinated FBI response to this nationwide crime problem by collating and analyzing information obtained from all available sources.

Today the FBI's Innocent Images National Initiative focuses on:

- Online organizations, enterprises, and communities that exploit children for profit or personal gain.
- Individuals who travel, or indicate a willingness to travel, for the purpose of engaging in sexual activity with a minor.
- Producers of child pornography.
- Major distributors of child pornography, such as those who appear to have transmitted a large volume of child pornography via an online computer on several occasions to several other people.
- Possessors of child pornography.

The FBI and the Department of Justice review all files and select the most egregious subjects for prosecution. In addition, the IINI works to identify child victims and obtain appropriate services/assistance for them and to establish a law enforcement presence on the Internet that will act as a deterrent to those who seek to sexually exploit children.

THE GROWTH OF THE INNOCENT IMAGES NATIONAL INITIATIVE:

Over the last several years, the FBI, local and state law enforcement, and the public has developed an increased awareness of the CP/CSE crime problem and more incidents of online CP/CSE are being identified for investigation than ever before. In fact, currently more personnel resources are expended towards violations worked under the IINI than any other program within the FBI's Cyber Division. Between fiscal years 1996 and 2003, there was a 2050% increase in the number of IINI cases opened (113 to 2430) throughout the FBI. It is anticipated that the number of cases opened and the resources utilized to address the crime problem will continue to rise.

The increase in Innocent Images investigations demonstrated the need for a mechanism to track subject transactions and to correlate the seemingly unrelated activities of thousands of subjects in a cyberspace environment. As a result, the Innocent Images case management system was developed and has proven to be an effective system to archive and retrieve the information necessary to identify and target priority subjects. All relevant data obtained during an undercover session is loaded into the Innocent Images case management system where it is updated, reviewed, and analyzed on a daily basis to identify priority subjects.

INNOCENT IMAGES NATIONAL INITIATIVE INVESTIGATIONS:

IINI undercover operations are being conducted in several FBI field offices by task forces that combine the resources of the FBI with other federal, state and local law enforcement agencies. Each of the FBI's 56 field offices has worked investigations developed by the IINI. International investigations are coordinated through the FBI's Legal Attaché program, which coordinates investigations with the appropriate foreign law enforcement. IINI investigations are also coordinated with Internet Crimes Against Children (ICAC) Task Forces, which are funded by the Department of Justice. Furthermore, IINI training is provided to all law enforcement involved in these investigations, including federal, state, local, and foreign law enforcement agencies.

During the early stages of Innocent Images, a substantial amount of time was spent conducting investigations on commercial online service providers that provide numerous easily accessible "chat rooms" in which teenagers and pre-teens can meet and converse with each other. By using chat rooms, children can chat for hours with unknown individuals, often without the knowledge or approval of their parents. Investigation revealed that computer-sex offenders utilized the chat rooms to contact children as a child does not know whether he or she is chatting with a 14-year-old or a 40-year-old. Chat rooms offer the advantage of immediate communication around the world and provide the pedophile with an anonymous means of identifying and recruiting children into sexually illicit relationships.

Innocent Images has expanded to include investigations involving all areas of the Internet and online services including:

- Internet websites that post child pornography
- Internet News Groups
- Internet Relay Chat (IRC) Channels
- File Servers ("FServes")
- Bulletin Board Systems (BBSs)
- Peer-to-Peer (P2P) file-sharing programs

FBI Agents and task force officers go online undercover into predicated locations utilizing fictitious screen names and engaging in real-time chat or E-mail conversations with subjects to obtain evidence of criminal activity. Investigation of specific online locations can be initiated through:

- A citizen complaint
- A complaint by an online service provider
- A referral from a law enforcement agency
- The name of the online location (such as a chat room) can suggest illicit activity

The FBI has taken the necessary steps to ensure that the Innocent Images National Initiative remains viable and productive through the use of new technology and sophisticated investigative techniques, coordination of the national investigative strategy and a national liaison initiative with a significant number of commercial and independent online service providers. The Innocent Images National Initiative has been highly successful. It has proven to be a logical, efficient and effective method to identify and investigate individuals who are using the Internet for the sole purpose of sexually exploiting children.

The National Center for Missing and Exploited Children (NCMEC) operates a CyberTipline at www.cybertipline.com that allows parents and children to report child pornography and other incidents of sexual exploitation of children by submitting an online form. The NCMEC also maintains a 24-hour hotline of 1-800-THE-LOST and a website at www.missingkids.com.

Complaints received by the NCMEC that indicate a violation of federal law are referred to the FBI for appropriate action. A FBI Supervisory Special Agent and four Investigative Analysts (IA) are assigned full-time at the NCMEC to assist with these complaints. The IAs review and analyze information received by the NCMEC's CyberTipline. The IAs conduct research and analysis in order to identify individuals suspected of any of the following: possession, manufacture and/or distribution of child pornography; online enticement of children for sexual acts; child sexual tourism; and/or other sexual exploitation of children. The IAs utilize various Internet tools and Administrative Subpoenas in their efforts to identify individuals who prey on children. Once a potential suspect has been identified, the IAs compile an investigative packet that includes the applicable CyberTipline reports, subpoena results, public records search results, the illegal images associated with the suspect, and a myriad of other information that is forwarded to the appropriate FBI field office.

INNOCENT IMAGES STATISTICAL ACCOMPLISHMENTS:

Between fiscal years 1996-2004 (2nd Quarter), the Innocent Images National Initiative has recorded the following statistical accomplishments:

| | |
|---|---|
| Number of Cases Opened | 11,855 |
| Number of Informations/Indictments | 3,358 |
| Number of Arrests/Locates/Summons | 3,682 |
| Number of Convictions/Pretrial Diversions | 3,316 |

The FBI's Innocent Images National Initiative is comprised of twenty-eight Under-Cover Operations. These operations involve FBI Agents on-line in an undercover capacity to seek child predators and individuals responsible for the production, dissemination, and possession of child pornography. This is accomplished by using a variety of techniques, to include purchasing child pornography from commercial web sites, creating on-line personas to chat in predicated chat rooms, and co-opting predators' e-mail accounts. Innocent Images has grown exponentially between fiscal year 1996 and 2003 with a 2050% increase in cases opened (113 to 2430). Between fiscal year 1996 and 2003, Innocent Images has recorded over 10,510 cases opened.

Recently, Peer-to-Peer networks were identified as a growing problem in the dissemination of child pornography. A GAO report published in September of 2003 indicated a four-fold increase in reports complaining of child pornography in Peer-to-Peer networks. In 2001, the FBI received 156 complaints about child pornography in Peer-to-Peer networks. By 2002, the number of complaints had risen to 757. This increase may be attributable to, among other things, the popularity of Peer-to-Peer networks, as well as the overall increase in child pornography available on the Intenet. These programs are free and are easy to install. In May of 2003, Sharman Networks, the developer of a very popular file sharing program, reported that their software had been downloaded more than 230 million times. This software and other file sharing programs like it, allow users to share files with anyone on the network. This creates an environment of relative anonymity amongst users however, this anonymity is only perceived, users are not truly anonymous.

Using Peer-to-Peer software, users' computers connect directly to one another to share files, without going through a central server. Nevertheless, each time a computer accesses the Internet, it is associated with an internet protocol, or "IP" address. Therefore, despite the fact that a Peer-to-Peer connection is not facilitated by a central server, users can still be identified in real time by the IP addresses associated with their computers.

IP addresses are the only way to definitively identify a particular user on a Peer-to-Peer network. In this environment, users of Peer-to-Peer often believe they are anonymous. There is some degree of truth in this assertion as peers in these networks are anonymous to each other. That being said, they are NOT anonymous to law enforcement. Through the use of covert investigative techniques and administrative subpoenas, Agents can determine which individual users possess and distribute child pornography over these networks. Utilizing search warrants, interviews, and computer forensic tools, Agents can strengthen their cases and these individuals are eventually indicted and prosecuted.

Agents have determined Peer-to Peer networks are one of many Internet havens for the open distribution of child pornography. Several of the individuals using Peer-to-Peer networks to distribute child pornography openly describe the content of the material they share as "illegal". This further contributes to the feeling of anonymity in these networks and leads users to become even more brazen in their conduct.

To combat this, the FBI has created an investigative protocol for Peer-to-Peer investigations to begin aggressively apprehending offenders. After developing a Peer-to-Peer investigative protocol with the Department of Justice's Child Exploitation and Obscenity Section , a number of cases were initiated to determine the techniques viability. Detailed discussion of these cases could possible jeopardize ongoing investigations, however, I would like to assure this subcommittee that the FBI is aggressively pursuing the trading of child pornography on Peer-to-Peer networks.

In these investigations, Agents have found child pornography to be readily available using the most basic of search terms. Often, child pornography was easily available when innocuous search terms were used, such as 'Brittney Spears' or the word 'young'.

Additionally, the FBI is exploring the possibility of working with Peer-to-Peer software clients to allow them to more effectively warn users against the possession, distribution, or production of child pornography. These industry members may also be interested in placing icons or a pop-up link from their home page regarding subjects wanted by the FBI for exploitation of children by use of the Internet.

While these efforts may not prevent someone from downloading the material in question, it will put the user on notice that they are, more than likely, violating the law. These efforts will also assist investigations as it will eliminate the ability of the subject to claim ignorance of the law.

In closing, the FBI looks forward to working with other Law Enforcement agencies, private industry, and the Department of Justice in continuing to combat this major crime problem. The protection of our children requires the combined efforts of all sectors of our society. I would like to thank Chairman Stearns and the committee for the privilege to appear before you and for your interest in this major crime problem.

Mr. STEARNS. Thank you.

Ms. Koontz?

## STATEMENT OF LINDA D. KOONTZ

Ms. KOONTZ. Mr. Chairman, members of the committee, thank you for inviting us to discuss our work on the availability of pornography on peer-to-peer networks. As it's been discussed, pornography, including child pornography, has become increasingly available as it has migrated from magazines, photographs and videos to the worldwide web. As you know, a great strength of the Internet is that it provides 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.

Today, I would like to discuss work we conducted last year at the request of the House Committee on Government Reform. Our results were summarized in a February 2003 report. This work focused on the availability of child pornography on peer-to-peer networks and on the risk of inadvertent exposure of juvenile users of peer-to-peer networks to pornography including child pornography.

In this work, we found that child pornography, as well as other types of pornography, is widely available and accessible through

peer-to-peer networks. We used Kazaa, a popular peer-to-peer file sharing program to search for image files using 12 key words that were known to be associated with child pornography on the Internet. Of over 1200 items identified in our search, about 42 percent of the file names were associated with child pornography images and about 34 percent with adult pornography images.

In another Kazaa search, we worked with Customs CyberSmuggling Center to use three key words 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.

More disturbing, we found that there is a significant risk that juvenile users can be inadvertently exposed to pornography including child pornography. In searches on three innocuous key words likely to be used by juveniles, we obtained images that included a high proportion of pornography. Almost half of the 177 retrieved images were classified as pornography, including a small amount of child pornography.

Mr. Chairman, Internet file sharing programs continue to be popular and while there are no hard statistics, it is thought that a large proportion of these users are juveniles. These programs provide easy access to pornography, including child pornography. Further, our work shows that the networks put even the youngest users at significant risk of being inadvertently exposed to pornography. In light of these factors, it will be important for law enforcement to continue to devote effort to peer-to-peer networks and for policymakers to continue to highlight this issue to parents and to the public and to lead the debate on possible strategies for dealing with it.

That concludes my statement. I would be happy to answer questions.

[The prepared statement of Linda D. Koontz follows:]

PREPARED STATEMENT OF LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GENERAL ACCOUNTING OFFICE

Mr. Chairman and Members of the Subcommittee: Thank you for inviting us to discuss our work on the availability of child pornography on peer-to-peer networks.

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).

My testimony today is based on our report on the availability of child pornography on peer-to-peer networks.[1] As requested, I will summarize the results of our work 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.

[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).

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

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 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 the dissemination of 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 fivefold—from 156 in 2001 to 840 in 2003.

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.

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

In the Child Pornography Prevention Act of 1996,[9] Congress sought to prohibit images that are or appear to be "of a minor engaging in sexually explicit conduct" or are "advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct." In 2002, the Supreme Court struck down this legislative attempt to ban "virtual" child pornography[10] in Ashcroft v. The Free Speech Coalition, ruling that the expansion of the act to material that did not involve and thus harm actual children in its creation is an unconstitutional violation of free speech rights. According to government officials, this ruling may increase the difficulty of prosecuting those who produce and possess child pornography. Defendants may claim that pornographic images are of "virtual" children, thus requiring

---

[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.

[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.

[7] See 18 U.S.C. § 2256(8).

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

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

[10] According to the Justice Department, rapidly advancing technology has raised the possibility of creating images of child pornography without the use of a real child ("virtual" child pornography). Totally virtual creations would be both time-intensive and, for now, prohibitively costly to produce. However, the technology has led to a ready defense (the "virtual" porn defense) against prosecution under laws that are limited to sexually explicit depictions of actual minors. Because the technology exists today to alter images to disguise the identity of the real child or make the image seem computer-generated, producers and distributors of child pornography may try to alter depictions of actual children in slight ways to make them appear to be "virtual" (as well as unidentifiable), thereby attempting to defeat prosecution. Making such alterations is much easier and cheaper than building an entirely computer-generated image.

the government to establish that the children shown in these digital images are real. Recently, Congress enacted the PROTECT Act,[11] which attempts to address the constitutional issues raised in The Free Speech Coalition decision.[12]

THE INERNET HAS EMERGED AS THE PRINCIPAL TOOL FOR EXCHAMGING CHILD PORNOGRAPHY

Historically, pornography, including child pornography, tended to be found mainly in photographs, magazines, and videos.[13] With the advent of the Internet, however, both the volume and the nature of available child pornography have changed significantly. The rapid expansion of the Internet and its technologies, the increased availability of broadband Internet services, advances in digital imaging technologies, and the availability of powerful digital graphic programs have led to a proliferation of child pornography on the Internet.

According to experts, pornographers have traditionally exploited—and sometimes pioneered—emerging communication technologies—from the dial-in bulletin board systems of the 1970s to the World Wide Web—to access, trade, and distribute pornography, including child pornography.[14] 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 sharina of diaital music, images, and video, peer-to-peer applications include BearSharig, Gndtella, LimeWire, and KaZaA. KaZaA is the most popular, with over 3 million KaZaA users sharing files at any time. |
| E-mail | E-mail allows the transmission of messages over a network or the Internet. Users can send E-mail to a single recipient or broadcast it to multiple users. E-mail supports the delivery of attached files, including image files. |
| Instant messaging | Instant messaging is not a dial-up system like the telephone; it requires that both parties be on line at the same time. AOL's Instant Messenger and Microsoft's MSN Messenger and Internet Relay Chat are the major instant messaging services. Users may exchange files, including image files. |
| Chat and Internet Relay Chat | Chat technologies allow computer conferencing using the keyboard over the Internet between two or more people. |

Source: GAO

Among the principal channels for the distribution of child pornography are commercial Web sites, Usenet newsgroups, and peer-to-peer networks.[15]

*Web sites.* According to recent estimates, there are about 400,000 commercial pornography Web sites worldwide,[16] 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

[11] Public Law No. 108-21 (Apr. 30, 2003).

[12] S. Rep. No. 108-2, at 13 (2003).

[13] 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)

[14] 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.planned parenthood.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.

[15] 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.

[16] 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/)

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,[17] they are emerging as a conduit for the sharing of pornographic images and videos, including child pornography. In a recent study by congressional staff,[18] 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.[19]

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 NCMEG.
[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 Ex-

[17] 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.

[18] 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)

[19] 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)

ploited Child Unit's CyberTipline II. The FBI, Customs Service, Postal Inspection Service, and Secret Service have staff assigned directly to NCMEC as analysts.[20]

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).[21]

The FBI investigates various crimes against children, including federal child pornography crimes involving interstate or foreign commerce. It deals with violations of child pornography laws related to the production of child pornography; selling or buying children for use in child pornography; and the transportation, shipment, or distribution of child pornography by any means, including by computer.

CEOS prosecutes child sex offenses and trafficking in women and children for sexual exploitation. Its mission includes prosecution of individuals who possess, manufacture, produce, or distribute child pornography; use the Internet to lure children to engage in prohibited sexual conduct; or traffic in women and children interstate or internationally to engage in sexually explicit conduct.

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

The Customs Service targets illegal importation and trafficking in child pornography and is the country's front line of defense in combating child pornography distributed through various channels, including the Internet. Customs is involved in cases with international links, focusing on pornography that enters the United States from foreign countries. The Customs CyberSmuggling Center has the lead in the investigation of international and domestic criminal activities conducted on or facilitated by the Internet, including the sharing and distribution of child pornography on peer-to-peer networks. Customs maintains a reporting link with NCMEC, and it acts on tips received via the CyberTipline from callers reporting instances of child pornography on Web sites, Usenet newsgroups, chat rooms, or the computers of users of peer-to-peer networks. The center also investigates leads from Internet service providers via the Exploited Child Unit's CyberTipline II.

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[22] showed that 543 (about 42 percent) of the images had titles and file names associated with child pornography images.[23] 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.

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).

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.

---

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

[21] 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.

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

[23] 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.

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 139,000 reports of child pornography, of which 76 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 45,000 in 2003—or about a thirty-two-fold increase. NCMEC did not track peer-to-peer referrals until 2001. Between 2001 and 2003, peer-to-peer referrals increased more than fivefold, from 156 to 840, reflecting the increased popularity of file-sharing programs.

Table 3: NCMEC CyberTipline Referrals to Law Enforcement Agencies, Fiscal Years 1998-2003

| Technology | Number of tips | | | | | |
|---|---|---|---|---|---|---|
| | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 |
| Web sites | 1,393 | 3,830 | 10,629 | 18,052 | 26,759 | 45,035 |
| E-mail | 117 | 165 | 120 | 1,128 | 6,245 | 12,403 |
| Peer-to-peer | - | - | - | 156 | 757 | 840 |
| Usenet newsgroups & bulletin boards | 531 | 987 | 731 | 990 | 993 | 1,128 |
| Unknown | 90 | 258 | 260 | 430 | 612 | 1,692 |
| Chat rooms | 155 | 256 | 176 | 125 | 234 | 786 |
| Instant Messaging | 27 | 47 | 50 | 80 | 53 | 472 |
| File transfer protocol | 25 | 26 | 58 | 64 | 23 | 13 |
| Total | 2,338 | 5,569 | 12,024 | 1,025 | 35,676 | 62,369 |

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's 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 were classified as nonpornographic.

## 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: Respurces Related to Combating Child Pornography on Peer-to-Peer Networks in 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.<br>$10 million for law enforcement training<br>$3.3 million for the Exploited Child Unit and the CyberTipline.<br>$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. |

Sources: GAO and agencies mentioned.
[a] Dollar amounts are approximate.
[b] Customs was unable to separate the staff hours devoted or funds obligated to combating child pornography from those dedicated to combating child exploitation in general.

An important new resource to facilitate the identification of the victims of child pornographers is the National Child Victim Identification Program, run by the CyberSmuggling Center. This resource is a consolidated information system containing seized images that is designed to allow law enforcement officials to quickly identify and combat the current abuse of children associated with the production of child pornography. The system's database is being populated with all known and unique child pornographic images obtained from national and international law enforcement sources and from CyberTipline reports filed with NCMEC. It will initially hold over 100,000 images collected by federal law enforcement agencies from various sources, including old child pornography magazines.[24] 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,[25] 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 child pornography. The increase in reports of child pornography on peer-to-peer networks suggests that this problem is increasing. As a result, it will be important for law enforcement agencies to follow through on their plans to devote more resources to this technology and continue their efforts to develop effective strategies for addressing this problem.

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

[24] According to federal law enforcement agencies, most of the child pornography published before 1970 has been digitized and made widely available on the Internet.
[25] 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.

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

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.[26]

The ability of peer-to-peer networks to provide services and connect users directly has resulted in a large number [27] of powerful applications built around this model.[28] 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,[29] 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 [30] network, in which individuals find each other and interact directly.

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,[31] which eventually led to its demise in September 2002.

In contrast to Napster, most current-generation peer-to-peer networks are decentralized. Because they do not depend on the server/broker that was the central feature of the Napster service, these networks are less vulnerable to litigation from copyright owners, as pointed out by Gartner.[32]

In the decentralized model, no brokers keep track of users and their files. To share files using the decentralized model, Ted starts with a networked computer equipped with a Gnutella file-sharing program such as KaZaA or BearShare. Ted connects to Carol, Carol to Bob, Bob to Alice, and so on. Once Ted's computer has announced that it is "alive" to the various members of the peer network, it can

---

[26] 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)

[27] 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)

[28] 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)

[29] 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).

[30] 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)

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

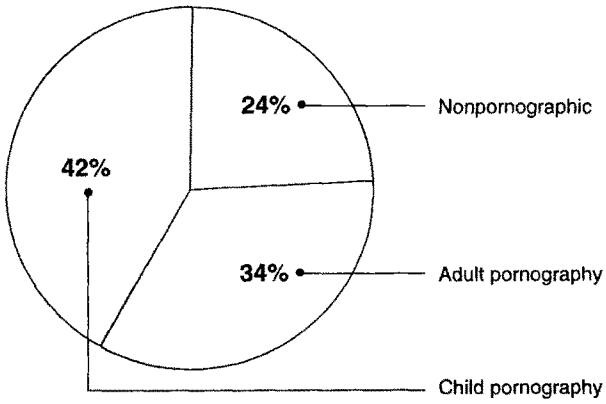
[32] Lydia Leong, "RIAA vs.Verizon, Implications for ISPs," Gartner (Oct. 24, 2002).

search the contents of the shared directories of the peer network members. The search request is sent to all members of the network, starting with Carol; members will, in turn, send the request to the computers to which they are connected, and so forth. If one of the computers in the peer network (say, for example, Alice's) has a file that matches the request, it transmits the file information (name, size, type, etc.) back through all the computers in the pathway towards Ted, where a list of files matching the search request appears on Ted's computer through the file-sharing program. Ted can then open a connection with Alice and download the file directly from Alice's computer.[33]

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.[34] 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.

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.[35] 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 a certain extent, preserve users' anonymity and provide information on whether a user is or is not connected to the Internet at a given moment. Peer-to-peer users thus may appear to be anonymous; they are not, however. Law enforcement agents may identify users' Internet addresses during the file-sharing process and obtain, under a court order, their identities from their Internet service providers.

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



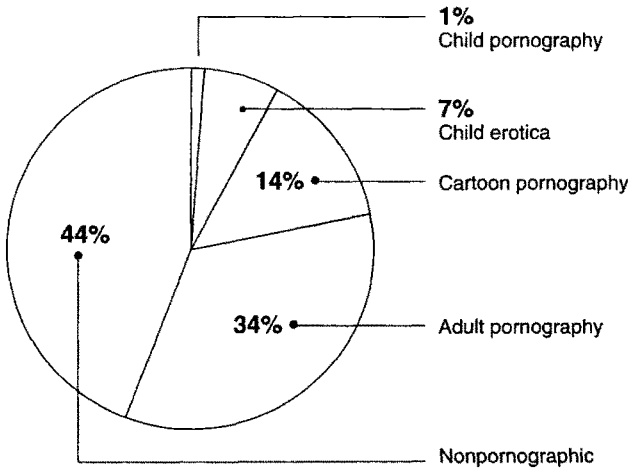

Source: GAO.

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

[34] 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)

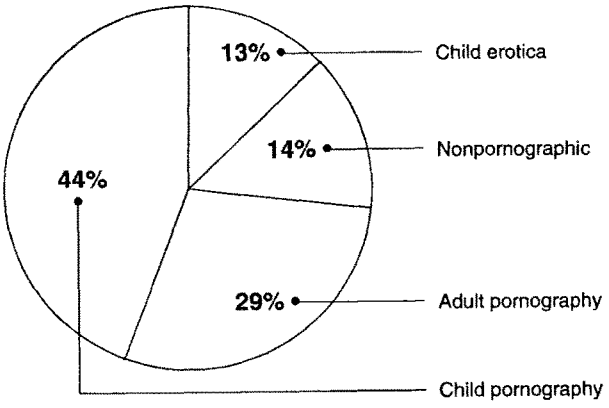
[35] S. Hayward and R. Batchelder, "Peer-to-Peer: Something Old, Something New," Gartner (Apr. 10, 2001).

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




Source: Customs CyberSmuggling Center.

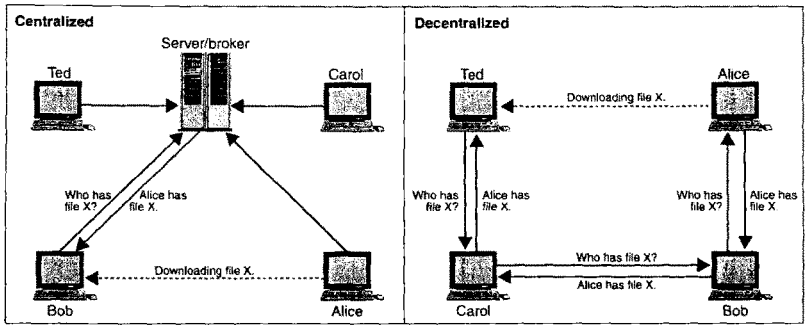
**Figure 2: Classification of 341 Images Downloaded through KaZaA**




Source: Customs CyberSmuggling Center.

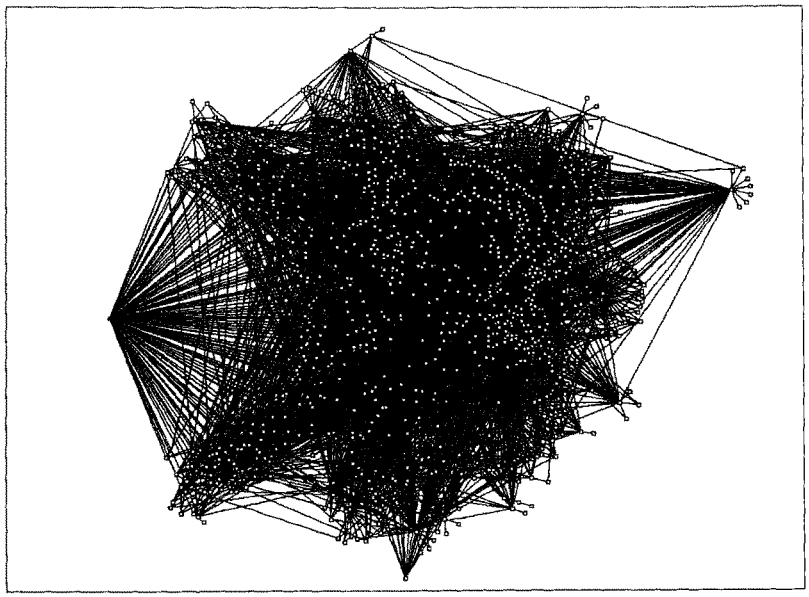
Note: GAO analysis of data provided by the Customs CyberSmuggling Center.

Figure 4: Peer-to-Peer Models




Source: Mark Bonnager, Bob Knighten.

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.

Mr. STEARNS. I thank you. By unanimous consent, Mr. John is recognized for an opening statement.

Mr. JOHN. Mr. Chairman, thank you very much. I certainly appreciate the latitude of Ranking Member Schakowsky and also Chairman Stearns for providing me an opportunity to give an opening statement. As a former member of this subcommittee and the lead sponsor of the legislation to protect children from online pornography, I really appreciate the opportunity to say just a few words.

I want to thank my fellow colleague, Congressman Pitts, for his leadership on this issue and offer my continued support for his efforts to combat child pornography. I also want to thank the panel. This is a little bit out of order to give an opening statement after the panel, but I certainly appreciate the remarks and a lot of the

remarks that I have in my opening statement were addressed or at least connected to some of your statements, so I certainly appreciate that.

As a parent of twin 5-year-old boys, I know the challenges that are faced by parents these days as kids go and log on to the Internet. In fact, my boys love to go on and log and look at Bay Blades and Yuggio cards and Power Rangers and a whole host of other kinds of kids-related shows and merchandise that are on these websites. And for the parents, it's a little difficult to keep up with some of these toys that kids today go a little crazy over. I guess what disturbs me more is the proliferation of pornography online that uses these very same kids' games, kids' toys, kids' characters to direct Internet users to pornography sites and a lot of the testimony cited that.

And it's all the more problematic when the kids are using the P2P or peer-to-peer file sharing programs because the names of these games and cartoons are often misspelled or look very similar in a lot of ways to some of these sites. We probably could spend an entire hearing, Mr. Chairman, on peer-to-peer file network, file sharing, as a digital means of stealing copyrighted material, but that battle will come and that's for another time.

But today, I appreciate the witnesses addressing some of the concerns that I have and I will continue my fight with Mr. Pitts on this issue and I thank the chairman and ranking member.

Mr. STEARNS. I thank the gentleman for his attendance. I'll start with my questions.

I guess the first question when you hear this, this is for the Federal Trade Commission, seeing what Mr. Pitts has showed us and going through some of the testimony on the panel, and hearing your example, I guess the question is do you have enough people? Do you need additional law enforcement support to curb the spread of online pornography via the Internet or the P2P?

Mr. BEALES. We can always do more with more resources. We have a very active program and I think one that's been very effective in addressing a wide variety of problems. It is—we don't have a particular request for additional resources. We'll address that through the appropriations process.

Mr. STEARNS. So you can say today that you think you have sufficient resources to handle this problem?

Mr. BEALES. Well, I think there is no amount of resources that would eliminate this problem.

Mr. STEARNS. We're not saying eliminate, but that you can get to the bad actors, that you feel comfortable that you can quickly and effectively get to these bad actors?

It seems to me if he puts up 6,000 sites, that's going to take a lot of research on your part and that's just one individual.

Mr. BEALES. Well, it's the way a lot of these cases work. He's got 6,000 sites registered under one name and once you're on to the basic scheme, tracking down all the other names he's registered is not that difficult. What's hard in some cases is finding the scheme in the first place.

Mr. STEARNS. Do you think there's anything we, as legislators, that you would recommend that we do?

Mr. BEALES. We don't have any legislative recommendations at this point.

Mr. STEARNS. So you have no opinion on the Pitts Bill?

Mr. BEALES. We have no position on the Pitts Bill. We have worked with Mr. Pitts' staff on technical issues and we look forward to continuing that.

Mr. STEARNS. Okay. Ms. Koontz, Mr. Lafferty has submitted written testimony. He's on the second panel. He stated that in using family filters at their maximum level, "no files retrieved on searches for popular terms like Britney, Pokeyman and the Olsen Twins will contain pornography."

Based on your work in this area, do you confirm his statement?

Ms. KOONTZ. I can't confirm that that's the case. We haven't done a study of the availability of pornography on the larger Internet sort of situation. So—and we have not studied the efficacy of filters either, although I would submit that we know that filters, although they can be helpful, are rarely perfect and usually do not eliminate all kinds of objectionable files.

Mr. STEARNS. Mr. Lourdeau or Mr. Beales, can you comment on that, the fact that Mr. Lafferty says basically the family filters work and they will prevent the pornography?

Mr. LOURDEAU. I have not checked out the filters to see if they work or not. I can't answer that.

Mr. STEARNS. Mr. Beales?

Mr. BEALES. We've not explored them in any detail either.

Mr. STEARNS. Let me ask the FBI, in which of the follow areas is child pornography most prevalent: Internet websites, Internet news groups, chat rooms, file servers, bulletin board systems or peer-to-peer file sharing programs? And also, to which area is it trending, if you can tell us that?

Mr. LOURDEAU. For the FBI, we have a priority listing of how we attack child pornography and as you said, Mr. Chairman, the websites is our No. 1 priority because of the international and national flavor of the websites. We think that the FBI's role is to try to go after organized groups that profit from child pornography and that occurs in the websites, where you can go into the websites and purchase child pornography and people make money from that.

Is it more pervasive than the other sites? I can give you countless examples of chat rooms where people go into chat rooms and discuss luring young children, girls and boys, to have sex with adults. So is it prevalent there? It's very prevalent there. I don't know if there's any one site or one——

Mr. STEARNS. Trending in any way?

Mr. LOURDEAU. [continuing] or trend that is more prevalent than the other. We know that there is a lot of legal file sharing of pornography over peer-to-peer networks and that's why we started our new initiative to address that crime problem.

Mr. STEARNS. Mr. Beales, the last question, are the P2P files traceable so that the illegal pornographers can be prosecuted? Is it easily traceable and has P2P software hastened the spread of spyware and adware?

Mr. BEALES. We have not been involved in circumstances where we needed to track back P2P files. That is not something that's come up in any of our cases and so I don't really know. We did

learn at our spyware workshop that a great deal of spyware and adware is distributed bundled with P2P networks. There are other distribution channels for it as well.

Mr. STEARNS. My time has expired.

Ms. SCHAKOWSKY. I'm afraid I don't really understand the technology, so you'll forgive me a little bit if I ask questions that are silly.

I'm looking now at Mr. Pitts' handout and when I look at Google which searches websites, am I correct about that? Okay, that when you search a website and the filter is in place, we find that there's no pornographic websites when you search for Cinderella.

When we look at Cinderella on this P2P network, I don't know what you call it, P2P file sharing, we get a lot of these pornographic information. So what I'm trying to understand is it a problem with the filtering system, I don't know what that implies, that there could be better blocking on the P2P or that the technology itself precludes that kind of blocking? And I wondered if one of you could answer that.

Mr. LOURDEAU. If I could just answer, maybe I could help out is that with peer-to-peer, when you share the files that go between one computer and another computer, individual computers, so it's not a file server that goes between. So to block out or use filters that would block one message from your computer to my computer that would not work.

Ms. SCHAKOWSKY. There's no possibility for doing that kind of filter?

Mr. LOURDEAU. I can't address if there is a possibility or not. I'm not a real technical person. So there might be some way to do that and again, I think that's private industry's position to come up with some type of block or filter to make that work.

Ms. SCHAKOWSKY. Let me ask you the question that the Chairman asked Mr. Beales. Are you able though to identify, I thought I heard you say that in your testimony, that you can identify the individual who does have this porn on their computer, on their e-mail that e-mails it. You can identify those individuals?

Mr. LOURDEAU. We've come up with a protocol and investigative technique that will identify individuals that are sharing child pornography through peer-to-peer. Again, that's part of our new initiative that we have on-going now, so I don't want to get into too much of that, that would jeopardize those investigations.

Ms. SCHAKOWSKY. Well, then let me ask you the question of whether you think there are enough legislative tools, legal tools for you to use or if you do think that we need more legislation that would help?

Mr. LOURDEAU. That's something I can review and get back with the subcommittee, if you allow me to. We're always looking for ways that would assist law enforcement in legislation and I'd be more than happy to again review anything that the subcommittee could help through legislation.

Ms. SCHAKOWSKY. Ms. Koontz, did you find that P2P is necessarily more risky than other means of accessing pron on the web? Or were you not comparing?

Ms. KOONTZ. Our study was focused on the availability of child pornography on peer-to-peer networks as well as the risk of inad-

vertent exposure to juvenile users. But that focused solely on the peer-to-peer networks. We did not try to compare either availability or inadvertent use to the Internet, to news groups or to any other kinds of technology. This was beyond the scope of what we were doing. However, we do note that we know that pornography is pervasive on these other mediums and that there is a risk of inadvertent exposure on them as well, but we can't do the quantitative comparison that you're asking about.

Ms. SCHAKOWSKY. Let me ask you this, do any of you feel that this will be the method of choice? You said that there's been, I think everyone said there's been an increase in the amount of pornography available through this P2P networks, but I'm wondering if that is not also true of all the others, of the websites, etcetera, or if we're seeing a trend now, this is going to be the way that seems easiest or most desirable for child predators or for purveyors of porn.

Mr. BEALES. Congresswoman, I think the factor that will limit expansion through this channel as opposed to others is that it's a lot harder to make money from it in the peer-to-peer context. In the website context, or in the e-mail context, you can try to sell people something and that's often a lot of the incentive to engage in the practice. You can't do that in the same way over the peer-to-peer networks and that's not to say it doesn't happen there, but it happens at a more individual level and not at a commercial level.

Ms. SCHAKOWSKY. The motivation though for someone then to use peer-to-peer might, in fact, be more the predators, rather than people who are seeking a profit might go there. Is that true?

Mr. LOURDEAU. I think it is true. Predators get on peer-to-peer networks and they know the terms to put in to obtain child pornography images, so that is true.

Ms. SCHAKOWSKY. I have a lot more to learn. Thank you.

Mr. STEARNS. Thank the gentlelady. The gentleman from Pennsylvania, Mr. Pitts.

Mr. PITTS. Thank you, Mr. Chairman. First of all, I want to thank the witnesses for their testimony. I want to thank the FTC for all they do and resources they offer to help consumers, especially parents, better understand the problems of pornography on the Internet and peer-to-peer.

Regarding the filters on the peer-to-peer systems in your opinion, Mr. Beales, do the filters provide clear and conspicuous information on how the filters work, filtering searches rather than content?

Mr. BEALES. I don't know that we've looked at that in detail as to exactly how they describe the use of the filter. We have looked at some of the filters and what we found is the way they work, as we understand it, is they just filter based on the file title or description, rather than on the full content of the file. I mean that would be unlike a web search engine which can look at the whole webpage and look at the content and not just the description.

Mr. PITTS. The FTC mission is to protect consumers against unfair and deceptive practices in commerce. According to the FTC an act is unfair if, among other things, the practice causes injury to consumers. Does a child inadvertently downloading pornography or even child pornography qualify as harm to a consumer?

Mr. BEALES. What we would typically focus on is how it happened. Tricking a child into doing that, there's no question that that's an unfair and deceptive act or practice and there's an injury in that kind of a context.

The nature of the injury that's involved in child pornography per se is really more of a criminal issue than something that's a typical FTC issue.

Mr. STEARNS. One of the dangers of peer-to-peer is when a person or a child accidentally downloads a pornographic file, if he or she immediately closes the file, but does not delete it, he or she becomes a distributor of that file, therefore a person can unknowingly become a distributor of child pornography. This, of course, could lead to legal problems for that individual.

Has the FTC looked into this aspect of peer-to-peer technology? Does this meet the threshold of an unfair practice?

Mr. BEALES. We have not looked into that at this point. It is again, if we're talking about something systematic where somebody is doing this on a large scale, to get kids to download images, that would certainly be something that we would be interested in that we think would be a violation.

There's one of our other recent spam cases is the Westby case and what it involved, and I think it's a good example of the kinds of things we're looking for in addressing this problem. This case involves spam with deceptive subject lines that try to trick you into opening the message and when you did, there were pornographic images. We think that was a deceptive practice. We think that's an unfair practice. We think it's a fairly straight forward case for us to make and it was in that particular instance, we prevailed in Court.

Mr. PITTS. Thank you. Mr. Lourdeau, with that illustration I gave, could you speak to how this complicates law enforcement efforts? There are probably thousands of people who are unknowingly distributing pornography out there.

Mr. LOURDEAU. And you're correct, sir. We have to prove intent and for the violation of the crime and for—that's one reason why the Bureau came out with a consumer letter that's posted on our website notifying the public of the dangers of peer-to-peer because of the bad potential, that if they are on the network sharing files between each other, that they are opening their systems up where somebody could come in and dump child pornography on their computers and that's one of the dangers of using the peer-to-peer programs.

Mr. PITTS. I think in your testimony you reference peer-to-peer software industry members that were considering placing icons or popups from home pages regarding subjects wanted by the FBI for exploitation of child on the Internet. Could you explain this concept a little bit more in detail?

Mr. LOURDEAU. Again, we work with a lot of different private industry companies because we have to because the technology is moving ahead so quickly, we need the cooperation of a lot of different private industries. We work with financial sectors. We work with ISPs. We work with companies involved in peer-to-peer software, just to help educate the public, also to give us the information we need to identify individuals that are using peer-to-peer.

We're in preliminary discussions with a number of different companies on how to again be more proactive and not just react to cases that come to the attention of individuals sharing child pornography and again, those are preliminary discussions and we haven't confirmed those yet.

Mr. PITTS. Thank you, Mr. Chairman, my time is up.

Mr. STEARNS. Mr. Terry.

Mr. TERRY. Mr. Beales, can you help me work through and explain the brown paper wrapper, in essence, putting some type of a mark out there that I would understanding that that particular file is—contains explicit images or content? Can you tell me how that would work in the area of peer-to-peer? Is there any overlap between our CAN-SPAM Act? Does it apply to the peer-to-peer fields that are posted? Is there something else that we need to do legislatively that would empower the FTC to force these peer-to-peer fields to be forthcoming in what the content is?

Mr. BEALES. I think the thing that's difficult about the peer-to-peer context is you're dealing with individual files labeled by individuals. And to go after those one at a time or to try to enforce brown paper wrapper kind of requirement one at a time, is something that would be exceedingly difficult to say the least. It's not like—because what you have is a single file or maybe a set of files, but it's from a single user who's posting those files on the Internet. And you'd be dependent on that individual to take the steps to comply with that requirement.

Mr. TERRY. Mr. Lourdeau, do you have anything to add from the FBI—do you agree that it is just too cumbersome, too large to go after individually? Is there anything that the FBI in that regard would require from us?

Mr. LOURDEAU. It is a massive problem and again, our new peer-to-peer initiative that we have underway addresses some of that and it's going to go after individuals who are sharing child pornography between each other and that's the initiative and again, in about 2 weeks I can speak more on that initiative.

Mr. TERRY. All right, in the Washington Post today there was a nice article that helped educate the public about peer-to-peer and its hazards. It also mentioned that the FBI is working with the BearShare, I think was mentioned and Kazaa had a whole separate paragraph to itself, which it should, considering that's probably one of the largest peer-to-peer sites or software.

Are there, is it true that Kazaa is quote unquote cooperating to make sure that you can find those who are sharing child pornography and are you able to tell us if there are some of those sites that aren't cooperating with you?

Mr. LOURDEAU. Again, we do cooperate with a lot of our industry partners because we have to. We need the cooperation of private industry to identify some of the subjects that are sharing files. The technology that the industry has and the access to information they have, the government does not have, so we need to cooperate with private industry.

We have had discussions with private industry on this technology and we welcome the shared knowledge that they have to help us address this crime problem. And to get into discussions of which in-

dustry partners are more cooperative than others, I don't know if this is the right forum for that.

Mr. PITTS. Okay. Is there a private forum that you would let us know which ones are not?

Mr. LOURDEAU. I'd be more than happy to give your staffers and yourself a briefing, yes sir.

Mr. PITTS. I appreciate that.

Mr. STEARNS. The gentleman yields back. Going to Mr. Ferguson, the gentleman from new Jersey.

Mr. FERGUSON. I have no questions, Mr. Chairman.

Mr. STEARNS. No questions. Next, Mr. Bass is not here. Go to Mr. Otter. No questions. Mr. Whitfield.

Mr. WHITFIELD. Mr. Chairman, I'll just ask one brief question. I was just curious, Ms. Koontz, whether or not you all had followed up since your 2003 report to look specifically at any new technologies incorporated into the P2P software?

Ms. KOONTZ. We have not.

Mr. WHITFIELD. Have not, okay. Thank you.

Mr. STEARNS. Thank the gentleman. Mr. Sullivan?

Pass. And Mr. Shadegg. Pass.

Before we go, I just want to ask Ms. Koontz, just a question. I understand the title of your GAO audit was "File Sharing Programs, Users of Peer-to-Peer Networks Can Readily Access Child Pornography." Is that correct?

Ms. KOONTZ. That's correct.

Mr. STEARNS. Is the risk of inadvertent exposure to pornography to children increasing on the Internet today? Just yes or no?

Ms. KOONTZ. I don't know.

Mr. STEARNS. Can you tell us is child pornography increasing on peer-to-peer, yes or no?

Ms. KOONTZ. It appears to be the case based on the number of tips forwarded to the National Center for Missing and Exploited Children. It appears to be the case, yes.

Mr. STEARNS. But in your actual study that you did, the GAO study, did not show that there's a trend increasing on peer-to-peer?

Ms. KOONTZ. Our study was at a point in time. We would have to sample at another point in time to tell you what that comparison was.

Mr. STEARNS. Do you intend to do that or not?

Ms. KOONTZ. If we are asked to do so, we will.

Mr. STEARNS. Okay. All right, I thank panel 1 and we'll now call for panel 2.

We have Mr. Charles Catlett, Senior Fellow, Computation Institute of Argonne National Laboratory. Mr. Martin Lafferty, Chief Executive Officer of Distributed Computing Industry Association. Mr. Norbert Dunkel, he's Director of Housing and Residence Education, University of Florida in Gainesville. Mr. Ernie Allen, President and Chief Executive Officer of the National Center for Missing and Exploited Children; and last, we have Ms. Penny Nance, President of Kids First Coalition.

So I welcome the second panel and thank you for your patience and time and we look forward to your opening statements and I think we'll start with Mr. Catlett, if you're ready to go.

Mr. Catlett has a demonstration for us, so I think we might need to turn down the lights a little bit, so that we can see it clearly on the television.

**STATEMENT OF CHARLES E. CATLETT, SENIOR FELLOW, COMPUTATION INSTITUTE, ARGONNE NATIONAL LABORATORY; NORBERT W. DUNKEL, DIRECTOR OF HOUSING AND RESIDENCE EDUCATION, UNIVERSITY OF FLORIDA; ERNIE ALLEN, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN; PENNY YOUNG NANCE, PRESIDENT, KIDS FIRST COALITION; AND MARTIN C. LAFFERTY, CHIEF EXECUTIVE OFFICER, DISTRIBUTED COMPUTING INDUSTRY ASSOCIATION**

Mr. CATLETT. Thank you, Mr. Chairman.

Mr. STEARNS. Get it right close to you. Sometimes these people drop their voice and then you can't hear them.

Mr. CATLETT. I've been working in the Internet for 20 years and I'm honored to be here and talk to you today about this. I'm also a father of three and these are things that concern me quite a bit, inappropriate material on the Internet.

I want to spent a little bit of time as a software and Internet expert telling you about some of the interesting things that we're doing on the Internet and specifically with distributed computing. I'm speaking as the Executive Director of the TeraGrid project which is funded by the National Science Foundation. We're building a distributed system with about 10 universities across the country. And I'm also the chair of an international group called the Global Grid Forum and this is about 200 organizations, 75 companies, worldwide. We develop specifications and standards for distributed software primarily for commercial and science applications.

Speaking of software, it's very difficult to classify software. We talk about distributed systems and that's any computer software that talks to another piece of software across a network. There are three kinds of distributed systems we generally talk about. One is client server. A client server system is like a web browser talking to a website.

Grid computing is what we talk about in the sciences because we want to combine resources that are not all available in one location, to be able to do an advanced application. I'll speak a little bit about three such applications.

And peer-to-peer tends to be desktop computers talking to one another and these tend to be much larger networks than the other, than the grid computing types.

One of the partners that we work with with our TeraGrid project is from the University of Oklahoma. This is the Center for Analysis and Prediction of Storms. And the goal of this project is to combine weather sensors that are Internet connected, doppler radar and things like that with super computers and data bases to be able to take our weather models and accelerate or increase the amount of time that citizens have available to them to take shelter in the case of a tornado or severe storms.

I live in Illinois. I'm told that the average time between a warning and the time you actually have to hit the cellar is 13 minutes.

With a program like that, we can increase that to an hour or 2 and actually predict the path of a tornado through a city like you see here. This is Fort Worth from 1998.

A second project is a medical project. This is very similar to peer-to-peer, but the content here is medical data, MRI data, protein data bases and the point of this project is to give people who are investigating brain diseases, give clinical researchers and academic researchers access to many more data bases than they might be able to have access to otherwise, do a single search, ask a complex query of 50 or 60 data bases that are federated or connected together using similar to peer-to-peer technology on the Internet. This is led by the University of California at San Diego.

And the third project is working with EPA and specifically the National Exposure Research Laboratory. We're investigating whether we can use the same technology that companies use to model say airflow over the body of a car, whether we can use that air flow model technology to model air flow through a city, an urban area. So if we could take a model of a city and we have data from a disaster, an explosion, a plume of smoke, toxins, airborne toxins, we're investigating the use of peer-to-peer and Internet technology to be able to bring that capability to the point where you might use it to guide emergency workers on the ground, if this plume of smoke is going to go this way and not that way.

I'd like to close with just a word or two about H.R. 2885, again, I appreciate being able to be here and talk to you about this because this is a concern I have as well. I think there's some very good ideas in this bill. The required warnings, standard notices for consumers allowing me as a consumer to make a choice about what the software is doing, not having some of the software that sneaks in and does things, I think that's excellent.

I would say also that in the Internet technology, 12 months is almost like a decade in other technologies and a lot can happen in 12 months. The language in this particular bill concerns me slightly because it's very broad and as I read it, it actually encompasses almost all of the software that is running on my computer right here. So I think with some precision, I think this would be very helpful and a strategy of working with software providers to actually harness the innovation and the technology that's available to combat this problem, I think is a very good approach. Thank you very much.

[The prepared statement of Charles E. Catlett follows:]

PREPARED STATEMENT OF CHARLES E. CATLETT, SENIOR FELLOW, UNIVERSITY OF CHICAGO AND ARGONNE NATIONAL LABORATORY CHAIR, GLOBAL GRID FORUM

Good morning, Mr. Chair and Members of the Committee. Thank you for allowing me this opportunity to comment on the use of the Internet and distributed computing technologies. I am Charles E. Catlett, a senior fellow at the Computation Institute at the University of Chicago and Argonne National Laboratory. I am the executive director of the NSF TeraGrid project, which is constructing one of the world's most powerful distributed computing systems, scheduled to be completed in October of this year. I am also the founding chair of the Global Grid Forum, an international standards body that brings together distributed computing researchers, commercial software providers, and end users to create software standards for distributed computing on the Internet. I have been involved in the evolution of the Internet since 1984, doing research in both advanced network technologies and the practical applications that these technologies enable. My work has been aimed at

providing increasingly powerful information technology tools for the science and education community.

I am also a father of three, and I pay very close attention to what my children are able to do with the Internet and Peer-to-Peer software in particular. I am very encouraged by your interest in these issues, which involve very complex technology and which have far-reaching impact on our Nation, and I am honored to speak with you about this technology.

I have prepared some brief remarks regarding what types of applications are possible with the increasing availability of broadband Internet and distributed computing software capabilities, and several examples of the kind of benefit we are seeing from these capabilities.

**1. Peer-to-Peer and "Grid" Computing**

Many terms have substantial overlap and cause confusion in discussions about the Internet and related software, so I would like to start with straightforward definitions of four such terms.

**"Distributed computing"** is a general term that refers to any set of computers that work together, using a network, to provide some form of capability. Most distributed computing software used on the Internet falls into three categories:

**"Client-Server"** computing involves a person using a program (a "client") on a home or office computer, interacting over a network with a larger computer, or "server." The server provides information, applications, or services to many clients. A Web browser is an illustration of a client, and the Google search site is an example of a server. Thus the Web is essentially a client-server system.

**"Peer-to-Peer"** could fairly be described as "client-to-client" computing, where the participating clients run on home or office computers, and where there may be tens of thousand or even millions of computers involved in sharing information or computing capabilities.

**"Grid"** is a term that is used increasingly often to refer to what we might call "server-to-server" computing. In a Grid system, shared resources such as powerful servers, databases, or scientific instruments are integrated to support applications that need powerful capabilities not available at a single location. Users of Grid systems may access them via client-server approaches.

All three forms of distributed computing share the Internet as their communications utility, and have many attributes in common. It is also difficult to classify many applications into only one of these three categories, because the most powerful applications tend to combine aspects of all three forms.

For this reason, it is important to consider a wide range of application types in order to determine the impact that would be felt with the introduction of regulations aimed at a particular software genre. This is not unlike the work that we do in the Global Grid Forum, where we consider the broader impact of any changes to a protocol or interface standard.

As with other Internet technologies such as the World Wide Web, it is difficult to predict what new applications will be enabled with new capabilities. Peer-to-peer technology is a good example, and in the research community we find a number of promising applications that are being developed and evaluated.

We see potential uses of "peer-to-peer" technology in many venues where information—whether scientific, clinical, or educational data—is shared among a large population of potential users. For example, the "OceanStore" project at the University of California-Berkeley is using peer-to-peer techniques to provide highly available, virtually "indestructible" storage systems that assume the underlying servers will be neither reliable nor secure. Groove Networks is a commercial software firm that uses peer-to-peer technology to create secure collaboration services for distributed teams, allowing individuals to work closely "together" despite being spread across many time zones. And many Grid applications share some aspects of peer-to-peer, as I discuss below.

**2. Practical Scientific Applications Using Distributed Computing Technologies**

I would like to focus on three applications of distributed computing technology. These are illustrative of the type of applications being developed on today's Internet, each of which uses a variety of distributed computing technologies. In each of these cases, peer-to-peer software has the potential for extending data sharing capabilities to a much broader audience than the current scientific collaborations, however none are using peer-to-peer software today.

The first involves predicting and response to severe weather, which causes hundreds of lost lives and some $13B in economic loss annually. Here I describe the work of Professor Kelvin Droegemeier, director of the Center for Analysis and Pre-

diction of Storms, and his colleagues. Weather applications are aimed at improving the nation's infrastructure for predicting and preparing for severe weather.

The second involves biomedical research aimed at understanding brain-related disease ranging from Alzheimer's to attention deficit disorder. Dr. Mark Ellisman, director of the Biomedical Informatics Research Network (BIRN), and collaborators at twelve U.S. universities are using the Internet to create highly secure, nationwide research and clinical data-sharing capabilities. The BIRN project uses the Internet and distributed computing and information technologies to create infrastructure aimed at improving biomedical research by enabling researchers throughout the United States to collaborate on large-scale studies of human disease with unique, multi-resolution tools. BIRN uses technology that is quite similar to peer-to-peer software, albeit with much greater control over security, access and authorization.

The third application is the analysis of urban air quality and airflow, seeking to understand the impact of both existing pollutants and potential effects of airborne toxins from events such as fires or explosions. This application includes the work of Dr. Alan Huber and colleagues from the Environmental Protection Agency's National Exposure Research Laboratory, Argonne National Laboratory's Environmental Assessment Division, and Fluent, Inc., a commercial software provider.

**2.1 Severe Weather Prediction and Early Warning**

The Center for Analysis and Prediction of Storms (CAPS) at the University of Oklahoma engages in basic and applied research in storm-scale data assimilation and numerical weather prediction, with several ongoing programs in collaboration with colleagues around the country. The work is aimed at integrating weather sensors and computer models, using high-performance computers and the Internet, to rapidly model evolving weather patterns in order to predict destructive storms in time to provide advanced warning.

Beginning in 1998, for instance, CAPS worked with the University Corporation for Atmospheric Research (UCAR) Unidata Program, the University of Washington, the National Severe Storms Laboratory (NSSL), and the WSR-88D Operational Support Facility (now the Radar Operations Center ROC) to establish the Collaborative Radar Acquisition Field Test (CRAFT) project. The goal of CRAFT was to demonstrate the real time compression and Internet-based transmission of NEXRAD data from multiple radars with a view toward nationwide implementation. CAPS is currently working with the National Weather Service to transition the CRAFT system into an operational service.

To further advance sensor capabilities, CAPS is working with the Center for Collaborative Adaptive Sensing of the Atmosphere (CASA) at the University of Massachusetts at Amherst, to revolutionize the remote sensing of the lower troposphere, initially via inexpensive, low-power, phased array Doppler radars placed on cell towers and buildings. A unique component of this project is that the sensors interact with one another, using the Internet to dynamically adjust their characteristics to sense multiple atmospheric phenomena while meeting multiple end user needs in an optimal manner. These communications and data sharing techniques are similar to what is typically classified as peer-to-peer.

Computer models have been used to predict long-term weather trends for several years. However, in order to predict severe weather with sufficient precision and in a time frame to allow for early warning, high-performance computing systems are essential. Several years ago CAPS developed computer-based storm prediction capabilities to identify severe thunderstorm activity with roughly 4 hours notice. This amount of time was sufficient, for example, to inform airlines of pending thunderstorms at major hubs, allowing those airlines to delay flights prior to takeoff in order to ensure that landing would be possible, greatly reducing the cost of diverting aircraft once in the air.

Today CAPS also leads an NSF-funded project called Linked Environments for Atmospheric Discovery (LEAD), which aims to create capabilities for analysis tools, forecast models, and data repositories to function as dynamically adaptive, on-demand systems. These systems will change configuration rapidly and automatically in response to the evolving weather, responding immediately to user decisions based on the weather problem at hand, and enabling the steering of remote observing systems to optimize data collection and forecast/warning quality. The goal of such systems is to provide precise information about the predicted path of destructive weather, such as tornados, in a timeframe that permits citizens to prepare for, rather than react to, such weather.

**2.2 Nationwide Sharing of Biomedical Research Data**

The Biomedical Informatics Research Network (BIRN) is an initiative sponsored by the National Institutes of Health (NIH) and National Center for Research Resources (NCRR). BIRN fosters large-scale biomedical science collaborations by utilizing emerging distributed computing technologies and the Internet, including applications distributed among high-performance computers, databases, and new software and data integration capabilities developed within the project and elsewhere.

The BIRN currently involves a consortium of 12 universities and 16 research groups participating in three testbed projects centered on the brain imaging of human neurological disease and associated animal models. Some

BIRN groups are working on large-scale, cross-institutional imaging studies on Alzheimer's disease, depression, and schizophrenia using structural and functional magnetic resonance imaging (MRI). Others are studying animal models relevant to multiple sclerosis, attention deficit disorder, and Parkinson's disease through MRI, whole brain histology, and high-resolution light and electron microscopy.

These studies are being used to drive the definition, construction, and daily use of a "federated data system." Federation presents biological data held at geographically separated Internet sites to appear as a single, unified and persistent data archive. Data is securely accessed across institutional boundaries to address issues of data privacy and automatic translation of data formats. Most of the groups participating in the BIRN have traditionally conducted independent investigations on relatively small populations, using site-specific software tools.

The promise of the BIRN is the ability to test new hypotheses through the analysis of larger patient populations and unique multiresolution views of animal models through data sharing and the integration of site independent resources for collaborative data refinement. To accomplish these goals, the BIRN project will continue to rely on innovative distributed computing technologies on the Internet.

**2.3 Air Quality and Impact of Airborne Biological or Toxic Agents**

Understanding the pathway of toxic air pollutants from source to human exposure in urban areas is of critical interest to the US Environmental Protection Agency, and has been an ongoing activity. Rapid assessments of risk, such as the migration of toxic gases related to major fires or chemical spills, are vital to first responders, local officials, federal officials, and the public. The scientific shortcomings are especially serious for incidents that occur in an urban center where the understanding of airflow around large buildings is poor.

Computational fluid dynamic (CFD) simulations have long been used in the aerospace and automotive industries to evaluate airflow around planes and cars, and increasingly in biomedical applications such as the modeling of blood flow through the heart. CFD techniques also have the potential to be employed to describe the flow of pollutants (be they a plume from an event such as an explosion or fire, or be they the dispersion of some pollutant or agent) in the complex terrain that our urban areas represent.

EPA scientists in the National Exposure Research Laboratory are working with Argonne National Laboratory's Environmental Assessment Division and Fluent, Inc. in a computational laboratory setting to test and use high fidelity CFD simulations of the spread and transport of contamination in urban building environments. In addition, the EPA-Argonne collaboration will also explore the possibility of developing or adapting the products from CFD simulations to support rapid exposure and risk models to potentially guide urban emergency response and emergency management for chemical, biological or radiological attacks or accidents.

As part of this investigation, EPA and Argonne scientists will use the Internet to exchange databases, simulation results, and other types of data. Experiments will be done using several forms of distributed computing on the Internet. One approach to be explored is the use of Fluent's Remote Simulation Facility, a Web-based "portal" that allows users to upload data from their computers to run a simulation on Fluent's computers. Another will be to use supercomputers at Argonne in client-server mode, and a third approach will attempt to couple Fluent's portal with supercomputers in NSF's TeraGrid project. All of these approaches are likely to be useful for some types of work, and some may employ technology that has functionality similar to peer-to-peer software.

**Concluding Remarks**

As a father and as a citizen I am very concerned about the availability of inappropriate material on the Internet. I would like to make several comments specifically regarding H.R. 2885.

The proposed requirements for *clear and prominent notice* would, in my view, be useful for software in general. Typical software end user license agreements are in-

comprehensible to average people. We have standard labels on food products to help consumers determine nutritional value, and dangers. A similar program for software could be designed to cover the disclosure proposed in H.R. 2885 as well as disclosure regarding privacy and security risks.

It is also very important to provide the user with clear and prominent notice regarding information sharing status and to require that *file sharing be explicitly enabled at the user's discretion,* not without their knowledge. Indeed some of the peer-to-peer software I have seen in recent months has already moved in this direction.

The proposed "do-not-install" beacon is an interesting idea, and I would encourage the committee to engage leaders from the software industry in exploring this idea and possible implementations.

I note that the H.R. 2885 definition for "peer-to-peer" software, as written, covers nearly all Internet software that I am aware of, including Web software, instant messaging software, and file transfer programs. In addition, the exclusion of software that is "marketed and distributed primarily for the operation" of networks implies that functionality built into computer operating systems (such as Windows or MacOS) would be excluded from these requirements. In practice, this would place a greater software engineering and support burden on small companies developing Internet software than would be placed on large companies adding new functions to operating systems software. This would put small software companies at a distinct disadvantage relative to their larger competitors.

In summary I would like to commend this committee for taking on this complex set of issues. I would also respectfully encourage the committee to engage leaders and experts from the software industry to work together toward achieving what I believe to be a common goal of protecting our children, and our privacy, while continuing to encourage innovation in this country using the Internet. This will require much more precision in the definition of the software to be regulated. Thank you very much for the opportunity to speak with you.

Mr. STEARNS. Thank you. Mr. Lafferty. Do you want me to take Mr. Dunkel and come back to you? That would be fine.

Mr. Dunkel, welcome. We'd like your opening statement, if you could.

**STATEMENT OF NORBERT W. DUNKEL**

Mr. DUNKEL. Thank you, Mr. Chairman, and members of the subcommittee. Good morning. I am Norb Dunkel, Director of Housing and Residence Education at the University of Florida. Thank you for the opportunity to appear before the subcommittee in order to provide you with information regarding the education of resident students and providing stewardship to our technological resources.

Many of you likely lived in a residence hall while attending college or university. Today's residence halls possess many, many more amenities and services than when I or you went to college. The electric typewriter that I brought was a hit to the guys on the floor. Well, now students are each bringing color TVs and stereo DVD players and refrigerators and videogame systems and desktop computers and laptop computers, along with their blackberry or cell phone or their PDA or other devices.

Now there are approximately 2 million students living in residence halls on campuses in the United States. One of the greatest additions to residence halls in the recent years is high speed ethernet connection. This high speed connection is used to support the institution's mission by allowing students to access online classes, replaying video classes, accessing class syllabi, signing up for classes online and the like. We are seeing connection speeds that only 6 or 8 years ago were the slow dial up modems to now 1,000 megabits which equals one gigabit connection.

As a comparison, with a dial modem it would take a person about 29 hours to download a 2-hour movie. With a gigabit connec-

tion, it takes about 6 seconds to download that same 2 hour movie. Downloading music files are inconsequential at that speed. The speed and efficiency is tremendous and will only get better and faster.

As housing professionals, we have two duties regarding the data connections we provide for residence students. First, we have a duty to educate our residence students as to the acceptable use of their computer and the network. Second, we have a duty to be good stewards in maintaining the technological infrastructure that we provide to students. Housing operations need to take an active role in educating residence students. A colleague and I recently found that 93 percent of institutions with high speed connections actively or passively educate their students. Some institutions, such as the University of Delaware, require students to take a responsible computing exam before they can obtain a network ID and password. The exam covers copyright resources, computer security, spam and harassing e-mail, bandwidth measurement and commercial and charitable use. The University of Hawaii in Manoa has residents sign for handbook accepting responsibility for reading and following the rules contained within.

At the University of Florida, residents register their computer online and electronically sign that they have read, understood and will abide by the policies governing acceptable use. For many students, this is all they will ever need. They will accept the policies and make no attempt to circumvent the policies. For other students, we need to be more active. To be good stewards of our technological infrastructure, my staff developed software to serve as a new network management program. We had to develop this software because the network could no longer support the academic needs due to high peer-to-peer volume. One tool available through this program mitigates peer-to-peer file sharing, while continuing to simultaneously educate students all while maintaining a network service free of illegal copyright sharing behaviors.

We wanted residents to understand that when they arrive on campus, and move into a residence hall, a new level of personal behavior and responsibility on the use of their computers and Internet would be expected. Most freshmen students arrive on campus having unabated access to the network. No knowledge of installing virus protection and they would allow anyone to use their computer. The education taking place on campuses stresses that students need to take responsibility for their computer and the use of their computer.

With me today is Mr. Rob Bird, the architect of the software program called ICARUS. I have sent you an advance, more detailed information on this program and its features, as well as the very successful outcomes. Rob is also available to answer your questions surrounding the technology and I would be happy to respond to your questions regarding the education. Thank you.

[The prepared statement of Norbert W. Dunkel follows:]

PREPARED STATEMENT OF NORBERT W. DUNKEL, DIRECTOR OF HOUSING AND RESIDENCE EDUCATION AND ROB BIRD, COORDINATOR FOR NETWORK SERVICES, DEPARTMENT OF HOUSING AND RESIDENCE EDUCATION, UNIVERSITY OF FLORIDA

I want to thank you for the opportunity to appear before the subcommittee to provide you information regarding the education of resident students and a new ap-

proach to mitigating Peer To Peer (P2P) file sharing. With me is Mr. Rob Bird the architect of the software program ICARUS which is an acronym for Integrated Computer Application for Recognizing User Services.

Many of you likely lived in a residence hall while attending a college or university. Today's residence halls possess many more amenities and services than when I attended Southern Illinois University at Carbondale. I came with a suitcase, box, and electric typewriter. The other students could not believe I had an "electric" typewriter.

There are approximately 2 million students living in residence halls on campuses in the United States. Today, students are moving into residence halls where suites and apartment style living is becoming increasingly available. The amenities that exist in residence facilities today include enhanced studying and recreational facilities; contemporary dining accommodations; and larger rooms with more storage to name a few. However, one of the greatest additions to residence halls is high speed Ethernet connection.

The primary purpose for providing Ethernet connection in residence halls is to support the academic mission. Many institutions, including the University of Florida, utilize this high-speed residential connection for on-line classes; accessing on-line services (i.e., class registration, room sign-up, ordering class textbooks, etc.); replaying video classes; accessing class syllabi; and working on group projects.

We have seen connection speeds grow in six or eight years from slow dial up modems to 10 MB to 100 MB to 1000 MB (1 Gigabit) speeds. As a comparison, with a dial up modem it would take a person about 29 hours to download a two hour movie. With a Gigabit connection, it takes about 6 seconds to download a two-hour movie. The speed and efficiency of this technology is tremendous.

As housing professionals, we have two duties regarding the data connections we provide to students. First, we have a duty to educate our resident students as to the acceptable use of their computer and the network. Second, we have a duty to be good stewards in maintaining the technological infrastructure that we provide students.

EDUCATION

In educating the resident students, we see many of our housing operations across the United States having integrated the academic community within the residential setting. Institutions have residence halls with live-in faculty, "smart" classrooms, faculty offices, space for tutoring, and space for academic advising. We see science-based (i.e., engineering, math, etc.); education-based (teaching, etc.); and fine arts-based (i.e., architecture, dance, theatre, etc.) residential academic communities. These types of arrangements and others lead to increased grade point averages for residents, increased graduation rates, increased respect for faculty, and increased psychosocial development. The education of our students is no longer taking place only in the classroom environment. The classroom environment is now in the residential setting.

Accompanying the residential academic environment is the need for housing operations to assist in the education of resident students on acceptable uses of the technology available to them. In an on-going study (J. Haynes and N.W. Dunkel, 2004), we have found that of the institutions surveyed with high speed connections in residence halls, 92% actively or passively educate their residents on the acceptable use of their computer and the Internet.

There exist a number of different approaches to this education. The information that is shared with residents may be as simple as defining terms and providing answers to frequently asked questions. The information may provide a general overview of the various aspects of a network and computer usage. At the University of Delaware, students must take a responsible computing exam before they can obtain a network ID and password. The exam covers copyright resources, computer security, spam and harassing e-mail, bandwidth measurement, and commercial and charitable use. At the University of Hawaii in Manoa, residents sign for the handbook accepting responsibility for reading and following the rules contained within. At the University of Florida, residents register their computer on-line and electronically sign that they have read, understand, and will abide by the policies governing acceptable use.

We know that for some students, reading the policies is all they will ever need. They will accept the policies and make no attempt to circumvent the policies. For other students, we need to be more active in our oversight and education.

STEWARDS OF TECHNOLOGY

Housing professionals must be good stewards of the technological infrastructure provided to students. The information that follows provides a summary of the ICARUS program developed by Mr. Rob Bird. ICARUS is a network management tool and one of the tools available is the mitigation of P2P file sharing.

*Introduction*

The University of Florida Department of Housing and Residence Education's Mission Statement is to provide well-maintained, community-oriented facilities where residents and staff are empowered to learn, innovate, and succeed. As staff worked to develop a software program to mitigate P2P file sharing, discussion continued on how to simultaneously educate resident students while maintaining a network service free of illegal copyright sharing behaviors. This was a daunting task as most first-year students arrive to campus having practiced P2P file sharing at home during their high school years. According to students, during high school years very little education on illegal file sharing was provided and student behavior remained unchecked. University of Florida housing staff wanted resident students to understand that when they arrive on campus, a new level of personal behavior and responsibility on the use of their computer would be expected.

*ICARUS*

ICARUS "pulls information from commercial and open-source tools used to monitor the network and spots traffic patterns that look like P2P transfers. ICARUS then tracks down the user's IP address, flashes a pop-up warning and limits its access to the internal campus network. An e-mail alert is sent to the student, who must agree to suspend use of the offending P2P desktop software to regain full Internet access" (p. 40, Network Computing). "There is no debate about ICARUS' effectiveness. Before it was turned on, there were as many as 3,500 simultaneous violators at any given time on the Gainesville campus, school officials say. On the day the switch was flipped, 1,500 violators were caught. There were only 19 second time violators and no third-time violators. Purged of the digital cholesterol of media files, the network saw an 85% drop in uplink data volume" (p. 42, Network Computing).

*Department of Housing and Residence Education Network Architecture—Technical*

The University of Florida Department of Housing and Residence Education computer network (DHNet) consists of Cisco Catalyst 4000/5000/6000-series switching equipment, and supports standards-compliant TCP/IPv4-services for its residents. The fully-meshed OC12 ATM LANE core network consolidates edge switches via OC3 & OC12 connections. A campus-wide VTP domain is maintained, managed by multiple central VMPS servers. Virtual LANs are deployed on a per-building basis to provide proper segmentation and encompass multiple levels of access granularity (Table 1). Specific services are subsequently provided by the UF DHNet and UF HRE web sites, depending on the source of access.

Table 1

| Access Level | Requires Registration? | Destination Restrictions? | Routed? | TCP/IP Services Provided? | DHNet web site role | Notes |
|---|---|---|---|---|---|---|
| Guest ..... | No | Yes | Yes | Yes, private IP addressing. | Network registration, computer configuration support and policy education. | Allows access to HRE registration & information sites only |
| Restricted .... | Yes | Yes | Yes | Yes, private IP addressing. | Judicial policy violation handling. Automatic recognition of restricted user. | Allows access to University resources only |
| Quarantine ... | Special | Yes | No | Yes, private IP addressing; DNS redirection; local web services via 802.1q trunks. | Distribution of tools, patches and updates. Automatic recognition of quarantined user. | Allows access to local network quarantine resources |

Table 1—Continued

| Access Level | Requires Registration? | Destination Restrictions? | Routed? | TCP/IP Services Provided? | DHNet web site role | Notes |
|---|---|---|---|---|---|---|
| Black Hole ... | Special | Yes | No | No ..... | None, no local or routed access provided. | Provided to leave systems actively connected for security analysis |
| Normal ..... | Yes | No | Yes | Yes, public IP addressing. | Network information, user forums, security, network policy and configuration information. | Typical user |
| Terminated .. | No Service | No Service | No Service | No Service ..... | No Service ..... | Last resort |

*Development and Deployment of ICARUS*

Beginning in December of 2002, the Department of Housing and Residence Education Network Services group initiated the development of a system to aid in the enforcement of its computer security policy. The system that was created was known as ICARUS, (Integrated Computer Application for Recognizing User Services).

ICARUS was designed to meet three primary design goals. First, to create a framework that allows for the collection of information from a variety of disparate sources so that the data can be evaluated and acted on in a unified fashion. Second, to create a system that allows for the real-time identification, containment, and education of managed network users while striving to minimize the impact on their academic use. Third, to leverage the use of GPL and BSD-licensed software, where possible. To this end, ICARUS consists of three main modules: (a) a data collection and parsing module intended to homologate information from SNMP, security tools, logging sources and non-traditional data sources such as debug output into a central database; (b) a data mining and analysis module which references external databases, performs signature analysis and other pertinent tasks; and (c) an action module that allows for the execution of any Perl-scriptable action.

Initial development of ICARUS focused on three core tasks. First, it was necessary to build a system for identifying users and tracking hardware movement within the network while allowing for the flexibility required of a residential system. The initial system comprised three levels of access and did not include a registration process for residents. While this system was adequate for private residence port authorization in light of the UF HRE judicial responsibility policy, it did not adequately support the use of public access ports, nor did it provide for a bulk way to handle the containment of security outbreaks. This solution was also deemed inefficient due to its heavy reliance on SNMP. Later, this system was expanded to six levels of access to address these additional operational requirements, and moved to leverage VMPS for superior access management. User registration was also added to more positively establish authorization without the use of network logon technologies, which are often cumbersome in "always-on" residential environments. Second, development was focused on containing P2P application use as an example of ICARUS' ability to detect and react to complex network management situations. By combining data from a variety of tools, it became possible to take a multi-faceted approach to application recognition. This approach allows ICARUS to react very quickly to both changing applications and policy requirements by removing reliance on a single application's ability to fully identify and contain unacceptable P2P use. In essence, it establishes a framework which allows for the ready automation of analysis and action that traditionally had to be performed with manual intervention. Third, development was focused on building Pearl actions for ICARUS to take, namely those involving VMPS, Windows Messenger Service, SMTP (internet email), and assorted SNMP actions. These actions were then customized to support the active network education plan created by HRE.

*Education of Resident Students*

The education of resident students takes place passively and actively. The passive educational program includes four steps: (a) Staff distributes an acceptable network use brochure during the check-in process. This brochure contains information on the overview of the housing network; relays the fact that housing aggressively enforces its ISP policies; briefs the student on servers, copyrights, and the DMCA; provides

information on the housing network monitoring and service restriction process; provides answers to frequently asked questions; and provides information on how student computer behavior is a part of the University of Florida Student Code of Conduct. (b) Staff places informational stickers by each housing data port. These informational stickers provide instructions to resident students on how to register on to the housing network. (c) The paraprofessional residence hall staff are trained prior to student check-in. These training sessions provide basic information so that staff are able to answer many of the student questions regarding the housing network. (d) The UF DHNet web site contains all the information regarding HRE Network Services. Students can read the information prior to their arrival at the University of Florida to understand what is expected and necessary when they register on to the housing network.

The active educational program designed by HRE is powered by ICARUS and supported by the UF DHNet and HRE websites. When ICARUS detects user activity deemed unacceptable by policy, an appropriate series of actions are performed. In the case of a violation of the HRE P2P policy, for example, the user in question is sent a notification pop-up message to their machine, a notification email to their official University email account, and all the computer systems owned by that resident are promptly restricted to campus-only network access (Table 2). This restriction is in effect regardless of where the resident physically goes within the HRE network, preventing abuse by those using public access ports. Simultaneously, an entry is created in the DHNet violation system, HAMMER. A snapshot of the user's activity, including all evidentiary data, is then added to the database, and correlated with past violations (if any). Residents are required to then visit the DHNet website in order to restore their access. When the resident visits the website with any of their computers, the page automatically recognizes them, and presents the resident with the list of violations. Instructions are provided for remedying each violation, and then a violation-dependent policy presentation is provided. Student violators are then presented with the terms of their restriction. It should be noted that the time counter for restriction does not officially begin until they have signed the on-line form with their University ID (access was still restricted before, however).

Table 2

| Violation Level | Duration of Campus-Only Restriction | Additional Requirements for Restoration |
|---|---|---|
| 1* | 0—Immediate restoration following completion of educational presentation. | None |
| 2* | 5 days | None |
| 3 | Indefinite | Meeting with the HRE Coordinator of Judicial Affairs |

*Special Handling Exception—Any resident with a prior DMCA complaint is automatically escalated to level 3 if the violation is sharing related in any way. Violators with new DMCA complaints are automatically level 3 for the purposes of ICARUS.

Residents who ignore the restriction and take no action automatically have their network access terminated after 10 days.

Similar action scenarios exist for a variety of situations from virus/worm quarantining to the active notification about available operating system patches to the active control of malicious activity.

*Outcomes of ICARUS Deployment*

The impact of ICARUS' deployment has been profound and immediate. Over the course of the six week Summer A term (608 Resident Users) and six week Summer B term (2435 Resident Users), 863 total P2P violations were detected and restricted by ICARUS. What is most striking, however, is the recidivism rate at each violation level for P2P use (Table 3).

Table 3

| Violation Level | Number of Violations | Recidivism Rate vs. Previous Level | Recidivism Rate vs. Total User Base |
|---|---|---|---|
| 1 | 769 | | 25.3% |
| 2 | 90 | 11.5% | 2.9% |
| 3 | 4 | 4.4% | 0.13% |

Additionally, ICARUS had a marked effect on overall internet bandwidth utilization. The HRE network experienced a drop in upload utilization of almost 83%. Per-

haps more impressive was the 3% increase in download utilization versus previous periods. Analysis demonstrated conclusively that the slight increase was due to people searching for, and finding, new legitimate sources of rich content. Furthermore, there was a notable increase in the viewing of online streaming video content.

I am pleased to provide you with this information. Housing professionals do have a responsibility to educate resident students on the acceptable use of their computers and the network. There exists numerous opportunities for students to use technology with legitimate purposes. Educating students to these purposes is part of our responsibility and stewardship.

**References**

Haynes, J., & Dunkel, N.W. (in process). P2P resident education in the United States.
Joachim, D. (2004, February 19). The enforcers. *Network Computing,* pp.40-54.

Mr. STEARNS. Thank you and we obviously want to welcome Rob here and if we have more technical questions on this software works relative to the dorms and how you filter it out, we'll be doing that.

Mr. Allen, I'll come to you next.

**STATEMENT OF ERNIE ALLEN**

Mr. ALLEN. Thank you, Mr. Chairman. In 1982, the Supreme Court of the United States said that child pornography was not protected speech, it was child abuse. And as a result, child pornography largely disappeared. It disappeared from the shelves of adult bookstores, the Customs Service crackdown on its importation, the Postal Service focused on its distribution through the mails. With the advent of the Internet, all of that has changed.

Since the advent of the Internet, we at the National Center have been operating the congressionally mandated CyberTipline. We have handled to date, 240,000 leads regarding child sexual exploitation; 215,000 of those leads have related to child pornography. In fact, we are convinced that its explosion on the Internet has been a direct result of the relative anonymity that a distributor or a trader could have online. And in fact, that's why we're so concerned about the problem with child pornography via P2P. We have handled, as was mentioned earlier, about 2100 reports. Now as a share of the 215,000, that's very low, but it's clear to us from anecdotal reports and discussions with law enforcement leaders around the world, that thousands of individuals are currently trading child pornography via peer-to-peer programs. And that these distributors could be found in every State and worldwide.

Why? Peer-to-peer programs make it more difficult to identify the users. In the past, we were able to easily identify offenders on the web because their Internet protocol of IP addresses were visible and they were required to reveal their e-mail addresses. That's no longer the case. When we receive P2P reports via our CyberTipline, it's almost impossible to identify the perpetrators responsible for trading the files. And law enforcement faces numerous challenges. There's no central data base of files, nor an organized network. There are no centrally held logs on these systems to record activity. Most of the popular file sharing programs are free, so there's no subscriber information available to subpoena to determine the user's true identity. Content and users change very rapidly. And this often requires law enforcement officers to be online at the very moment that the offense occurs.

As Keith Lourdeau from the FBI mentioned earlier, tracking users trading illegal content on peer-to-peer is difficult, but not im-

possible. Savvy computer users can use certain commands to attain an IP address of a user sending a file. Also, proactive law enforcement agencies have begun to use secondary programs to identify the IP address of the perpetrator sharing the illegal files. However, these programs must be active at the exact moment of the file transfer and depending on the particular peer-to-peer program, if a user accidentally downloads an illegal file, there is no way for that user to document where the file originated. Considering the massive amounts of files being shared at any given moment, this anonymity provides a cloak of security for those criminals trading images of children being sexually abuse.

In our judgment, the extensive swapping of child pornography images on peer-to-peer would be reduced if users knew that recipients of the images or movies could easily attain their IP address.

Mr. Chairman, we don't come here today with quick, easy solutions, but it is our conclusion that the use of peer-to-peer networks for the distribution of child pornography is growing dramatically and further, we suspect that it will continue to increase as child pornographers search for lower risk avenues where the possibility of being identified is far less.

Federal, State and local law enforcement are more aggressive on this issue than ever before, but they face significant barriers. I hope you can help us remove some of those barriers and help us identify and prosecute those who are misusing the Internet and misusing a very positive technology resource for criminal purpose.

Thank you, Mr. Chairman.

[The prepared statement of Ernie Allen follows:]

PREPARED STATEMENT OF ERNIE ALLEN, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Mr. Chairman and members of the Committee, I am pleased to appear before you today and express the views of the National Center for Missing & Exploited Children (NCMEC) regarding the issue of Peer-to-Peer networks and the distribution of child pornography.

Let me first provide the Committee with some general background on NCMEC and why we are so concerned about this issue. NCMEC is a not-for-profit corporation, mandated by Congress and working in partnership with the U.S. Department of Justice as the national resource center and clearinghouse on missing and exploited children. NCMEC is a true public-private partnership, funded in part by Congress and in part by the private sector. NCMEC's federal funding supports specific operational functions mandated by Congress, including a national 24-hour toll-free hotline; a photo distribution system to generate leads regarding missing children; a system of case management and technical assistance to law enforcement and families in the search for and recovery of missing children; training programs for federal, state and local law enforcement; and much more.

While we are perhaps best known for our work in the field of missing children, NCMEC is also a leader in the battle against child sexual exploitation and has become the epicenter of the war against child pornography. How did we become such a central figure in the child pornography battle?

- The Child Porn Tipline was launched in June 1987 as a service for the U.S. Customs Service and subsequently for the U.S. Postal Inspection Service. In partnership with the U.S. Customs Service and U.S.P.I.S., NCMEC has received and processed 11,000 such leads.
- In 1994, months before the nation or the news media viewed online victimization as a problem, NCMEC first printed the brochure, "Child Safety on the Information Highway," a publication discussing online child safety. Subsequently, a number of children were lured away to meet adults they'd met online, and suddenly online victimization became front-page news. Because we were the only child advocacy group at the time with solid tips on how to prevent online victimization, the news media and families turned to NCMEC for help.

- On January 31, 1997, in response to the increasing prevalence of child sexual victimization, NCMEC officially opened its Exploited Child Unit (ECU). The ECU is responsible for receipt, processing, initial analysis and referral to law enforcement of information regarding the sexual exploitation of a child.
- In 1997 the Director of the FBI and I testified before the Senate Appropriations Subcommittee on Commerce, Justice, State and the Judiciary. The committee asked how serious was the problem of Internet-based child sexual exploitation. Director Freeh and I agreed that it was a serious and growing problem that we were just beginning to recognize and address, and that much more needed to be done at the federal, state and local levels. As a result of that hearing, Congress directed NCMEC to establish an Internet-based, reporting mechanism for child pornography, online enticement of children, child molestation, child prostitution and child sex tourism. Congress also directed the Justice Department to establish multi-jurisdictional Internet Crimes Against Children Task Forces across the country.
- On March 9, 1998 NCMEC launched its new CyberTipline, www.cybertipline.com, the "911 for the Internet," to serve as the national online clearinghouse for investigative leads and tips regarding child sexual exploitation. NCMEC's CyberTipline is linked via server with the FBI, Homeland Security's Bureau of Immigration and Customs Enforcement (ICE) and the Postal Inspection Service. Leads are received and reviewed by NCMEC's analysts, who visit the reported sites, examine and evaluate the content, use search tools to try to identify perpetrators, and provide all lead information to the appropriate law enforcement agency and investigator. The FBI, ICE and Postal Inspection Service have "real time" access to the leads, and all three agencies assign agents who work directly out of NCMEC, and review reports. The U.S. Secret Service has assigned three analysts who assist in the review and prioritization process. The results: to date (through May 2, 2004), NCMEC has received and processed 237,147 leads, 215,599 of which were reports of child pornography, resulting in hundreds of arrests and successful prosecutions.
- In December 1999, Congress passed the *Protection of Children from Sexual Predators Act,* mandating that Internet Service Providers report child pornography on their sites to law enforcement, subject to substantial fines for failure to report. Again, Congress asked NCMEC if it could handle the reports through its CyberTipline. NCMEC agreed. While the reporting mechanism is being formalized, NCMEC has entered into agreements with 122 major ISPs, including industry leaders America Online and the Microsoft Network, who are already reporting child pornography on their sites voluntarily.
- Currently, NCMEC receives and analyzes CyberTipline leads in seven categories, the final category added as a result of passage of the PROTECT Act in 2003:
  - possession, manufacture, and distribution of child pornography;
  - online enticement of children for sexual acts;
  - child prostitution;
  - child-sex tourism;
  - child sexual molestation (not in the fam)ly);
  - unsolicited obscene material se.t to a child; and
  - misleading domain names

Today, NCMEC is receiving hundreds of reports and tips re#arding child pornography from across America and around the world each week, and it is pursuing those leads agressively with the appropriate law enforcement agencies. We are proud of the progress. Following the Supreme Court's 1982 Ferber v. New York decision holding that child pornography was not protected speech, child pornography disappeared from the shelves of adult bookstores, the Customs Service launched an aggressive effort to intercept it as it entered the country, and the U.S. Postal Inspection Service cracked down on its distribution through the mails. However, child pornography did not disappear, it went underground.

That lasted until the advent of the Internet, when those for whom child pornography was a way of life suddenly had a vehicle for networking, trading and communicating with like-minded individuals with virtual anonymity and little concern about apprehension. They could trade images with like-minded individuals, and in some cases even abuse children "live," while others watched via the Internet.

However, in recent years law enforcement began to catch up, and enforcement action came to the Internet. The FBI created its Innocent Images Task Force. The Customs Service expanded its activities through its Cyber Crimes Center. The Postal Inspection Service continued and enhanced its strong attack on child pornography. The Congress has funded forty Internet Crimes Against Children Task Forces at the state and local levels across the country. Child pornography prosecu-

tions have increased an average of 10% per year in every year since 1995. We were making enormous progress.

On the subject of today's hearing, the trading of child pornography via peer-to-peer networks, NCMEC's Cyber Tipline has received 2,100 reports. However, we are convinced that is in no way descriptive of the real scope of the problem. Through anecdotal reports and conversations with law enforcement officials across the country, it is clear to us that thousands of individuals are trading child pornography via peer-to-peer programs, and that the people utilizing this method of distribution can be found in every state and in countries around the world.

Peer-to-peer programs have made it more difficult to identify the users. In the past we were able to easily identify offenders trading child pornography using peer-to-peer programs because their Internet Protocol (IP) addresses were visible and they were required to reveal their email addresses. This is no longer the case. When we receive reports to the CyberTipline, it is almost impossible to identify the perpetrators responsible for trading the illegal files. The anonymity of recent peer-to-peer technology has allowed individuals who exploit children to trade images and movies featuring the sexual assault of children with very little fear of detection.

Law enforcement agencies face numerous challenges including:

- There is no central database of files nor organized network
- There are no centrally-held logs on these systems to record activity
- Most of the popular file-sharing programs are free so there is no subscriber information available upon subpoena to determine the user's true identity
- These are dynamic systems where content and users change very rapidly. This often requires law enforcement officers to be online at the very moment the offense occurs.
- Individuals from all over the world use these peer-to-peer programs.

While tracking users trading illegal content on peer-to-peer has become increasingly difficult, it is not impossible. Savvy computer users can use certain commands to attain an IP address of a user sending a file. Also, several proactive law enforcement agencies have begun to use secondary programs to identify the IP address of the perpetrator sharing the illegal files.

However, these programs must be active at the exact moment of file transfer. Depending on the particular peer-to-peer program, if a user accidentally downloads an illegal file, there is no way for that user to document where the file originated. Considering the massive amounts of files being shared at any given moment, this anonymity provides a cloak of security for those criminals trading images of children being sexually abused.

It is quite likely that the extensive swapping of child pornography images on peer-to-peer networks would be reduced if users knew that recipients of the images/movies could easily attain their IP address.

At NCMEC we have had some success when we learn about child pornography trading via peer-to-peer networks. Let me cite two recent cases where there was a successful resolution from peer-to-peer CyberTipline reports:

- The CyberTipline received an anonymous complaint about a website in which one could share media files using a peer-to-peer network. The reporting person indicated that images of child pornography were available on this site. NCMEC analysts found numerous images of child pornography and determined that one of the suspects posting and distributing child pornography was using an IP address registered to the University of California. NCMEC analysts contacted Campus Police. Because the images were found on the peer-to-peer network, detectives were initially unable to locate the images because the suspect was offline. As a result, analysts worked with a university detective and assisted in locating the images.

  Subsequently, university detectives, working with detectives from the Santa Barbara Co. Sheriff's Department High-Tech Crime Unit, were able to verify the existence and location of the operation. A 21-year old suspect was identified and detectives executed a search warrant at his apartment located off campus and seized his computer. A forensic search of the computer found numerous child pornography images. The suspect confessed and the District Attorney's Office filed felony charges of distributing child pornography.
- NCMEC received a CyberTipline report indicating that a suspect was offering child pornography through a peer-to-peer program. This reporting person was highly skilled with computers and used commands to document the IP address of the person trading the child pornography images. Using detailed information provided by the reporting person, ECU analysts determined that this IP address originated in Kansas.

NCMEC contacted Kansas law enforcement officials and provided documentation of the suspected illegal files being traded. The police apprehended the suspect and charged him with 500 counts of possession/distribution of child pornographic material, sexual exploitation of a child, and indecent liberties with a child. The suspect admitted to raping, sodomizing and sexually abusing his own daughter.

It is unlikely this predator would have been arrested if a concerned citizen hadn't known the steps to take when she accidentally received one of his images. It is troublesome to imagine the number of offenders who are not reported because the average citizen does not know how to collect the necessary information. Peer-to-peer program developers could make great strides in protecting children if they allowed the software programs to allow users to log the origination of files.

Mr. Chairman, I don't come before you today with a quick, easy solution to this problem, but I can state unequivocally that the problem of illegal child pornography has exploded with the advent of the Internet and that the use of peer-to-peer networks for the distribution of child pornography is growing dramatically. Further, we suspect that it will continue to increase as child pornographers search for lower risk avenues where the possibility of being identified is far less.

Federal, state and local law enforcement are more aggressive than ever before, but they must overcome significant barriers. I hope that you can help us remove some of those barriers and help us identify and prosecute those who are misusing the Internet for insidious, criminal purposes. Too many child pornographers feel that they have found a sanctuary, a place where there is virtually no risk of identification or apprehension.

In the area of peer-to-peer dissemination of child pornography, I fear that we have only scratched the surface. Far more must be done. NCMEC is willing and eager to play an even larger role in addressing this problem.

Mr. STEARNS. Thank you, Mr. Allen. Thank you for all that you do.

Ms. Nance, welcome.

**STATEMENT OF PENNY YOUNG NANCE**

Ms. NANCE. Thank you, gentleman and ladies, for convening this hearing. It's very important. I appreciate it.

My name is Penny Nance, I'm the President of the Kids First Coalition which is a nonprofit educational and advocacy group.

Mr. STEARNS. Penny, I'm going to have you move it just a little closer.

Ms. NANCE. That I founded with the idea of protecting children and families. I sit before you not only a pro-family advocate, but also a mother of two small children and also as a victim of attempted rape by someone who was deeply involved in pornography.

I also represent Concerned Women for America Today who has over 500,000 members across the country and I have with me the Salvation Army, American Association of Christian Schools, it's a broad group of pro-family people who really feel strongly about this issue.

Most of you are probably unaware from May is Victim of Pornography month and I guess it's sadly no more appropriate than we discuss this issue at this time.

Today is the wild west of the Internet with an estimate by Forbes Magazine of $1.5 billion in global sales per year. One must understand exactly what defines hard core pornography and obscenity that are on these kind of sites. It's not Playboy. It encompasses depiction of bestiality, bondage, domination, gang rape, urine and excrement, sexual murders, child sex and torture. It's vile and it's hurtful. It is not loving and sexy. And all of it is just

a click away from our kids. We as parents know instinctively that simply viewing pornography of any kind can be damaging to children.

Illegal obscenity is overwhelming available on the internet and a long with this vile image await large numbers of disturbed individuals, huge strides in this area.

Thank you for allowing me to testify today.

[The prepared statement of Penny Nance follows:]

PREPARED STATEMENT OF PENNY YOUNG NANCE, PRESIDENT, KIDS FIRST COALITION

Hello, my name is Penny Nance and I am the President of Kids First Coalition, which is a non-profit educational and advocacy group I founded with the goal of protecting children and advancing pro-family legislation. I sit before you not only as a pro-family advocate but also a very concerned mother of two young children and a victim of an attempted rape that was connected to pornography. I am sincerely passionate about this issue. Most of you probably are unaware but May is "Victims of Pornography Month" and a sadly appropriate time to discuss Internet safety.

Today is the wild west of the Internet with an estimate by Forbes of $1.5 billion in global sales per year. One must understand what exactly defines hard-core pornography or obscene material on the Internet. It's not Playboy! It encompasses the depiction of bestiality, bondage, domination, rape, gang rapes, urine and excrement, sexual murders, child sex and torture. It is vile and hurtful, not sexy and loving. And all of it is just one click away from our kids. We as parents know instinctively that simply viewing pornography of any kind can be damaging to children.

The 1986 Meese Commission on Pornography, and countless law enforcement and behavioral scientists say there is a direct link between pornography and sexual violence. My experience of attempted rape by a strange man deeply involved in pornography confirms this belief. A topic for another day is the undeniable connection between pornography and violence against women and children.

Today, I am here to represent the members of my organization, (mostly moms who have downgraded professional careers to raise kids) as well as the countless parents in this country who seek to protect their children from graphic sexual images on the Internet.

Although this hearing today is centered on peer-to-peer pornography, Kids First Coalition is also concerned about all types of Internet pornography and the safety of children. We have worked to combat this pervasive problem in a number of areas including advocacy for Truth in Domain names, tighter laws on porn spam, a ban of virtual child porn and better enforcement of current law.

Kids First Coalition has worked closely with the Bush administration and the Department of Justice to urge a reversal of the Clinton Administration's policy to ignore obscenity crimes on the internet. I am pleased to say that DoJ listened and is currently actively prosecuting cases that four years ago would have gone unnoticed. We urge each of you to support the President's Budget which contains about $33 million and about $13.8 million in new funds to specifically pay for law enforcement. The budget contains $14.5 million for the Internet Crimes Against Children (ICAC) program, which helps state and local law enforcement agencies develop effective responses to Internet child enticement and child pornography cases. It also contains $3 million for the Innocent Images National Initiative, which will support existing Innocent Images undercover operations and investigations designed to ferret out child predators.

Illegal obscenity is overwhelmingly available on the internet. And, along with these vile images await large numbers of disturbed individuals seeking to prey on our children. Predators lurk in chat rooms, instant messaging, websites and peer to peer sites. Today's parents must be more vigilant in protecting the safety and innocence of their children then ever before in our history.

Most children are not looking for pornography, but far too often pornography is looking for them. Pornography will come uninvited and unannounced into your home and will prevail upon your unsuspecting children the moment you turn your back even for a second. The Kaiser Family Foundation found that 70 percent of online youth between the ages of 15-17 say they have stumbled across pornography online, and of those exposed to such content, 49 percent were upset by the experience. The study also found that young people agree: "[Stumbling upon pornography] is upsetting to many young people—especially young girls—and most think it is a serious problem."

The most common ways kids stumble into porn is by innocent searches on computers without filter. Pornographers use misspelled search terms to lure young people into their sites. The pornography industry was way ahead of Joe Camel in working to addict customers at an early age.

Fortunately, most internet service providers are actively working to provide both filters that shield kids from viewing explicit materials and closed systems that would disallow kids to even enter parts of the internet. Protectkids.com is a great resource for parents to educate themselves on safety resources. Unfortunately, most estimates show that about half of all family computers lack any safety precautions.

And those parents that do utilize filters may still not be doing enough to protect their kids. Peer to peer computer sites do not use a central server so normal filtering will not keep kids out.

They are a source of serious concern to American parents. I've spoken to hundreds of concerned parents around the country, and conducted over fifty radio interviews on this subject, I have discovered that peer-to-peer networks are a place where unsuspecting kids can access pornography far too easily.

As a way of background, peer-to-peer networks are programs that allow computer users to share electronic files with one another, usually in the form of downloading free music or images. KaZaA is the most popular site (with over 4 million users at any one time) but other sites include Grokster, Morpheus, and Gnutella. While many parents assume their children are downloading free, non-offensive music or images on these networks, in actuality these children can be in direct contact with child and adult pornography and sexual predators. A recent GAO study said that kids searching with innocent keywords like Britney Spears or Pokemon would find either graphic adult pornography or child pornography 56% of the time. (This report is available on gao.gov, report number GAO-03-351).

The owners of peer to peer sites like to say that only a fraction of the child and adult porn available on the Internet exist on their sites. This doesn't absolve them of the problem nor does it take into account some factors that make peer to peer sites in some ways more dangerous than the Internet overall. As one dad told me, "On Google you have to ask to see something. On Kazaa, you ask for Elmo and they push porn at you . . ."

1) According to a GAO study, normally Internet users must actually pay to view pornography (using a credit card), but peer-to-peer sites are generally free.

2) since peer-to-peer files do not go through a center server, most child-protection filters are ineffective and the filters on the peer-to peer sites are flimsy and can be easily dismantled by computer-savvy kids, and

3) Most importantly, these sites are considered hip and popular places for kids to go and are therefore more heavily visited by children. According to the GAO, 4 million people are on Kazaa alone at any one time and 40% of those are kids. Therefore about 1.6 million kids are on KaZaa at any one time and who knows about all the other sites.

Pedophiles are not ignorant of this. What is more alarming is that instant messaging is also available on these networks, which gives easy access to child predators to communicate with unsuspecting children. Pedophiles can pose as kids in order to begin a dialogue with children on-line.

Let me walk you through a scenario that will help you to understand what is happening in America numerous times every day. Jenny is a spunky ten-year-old who is sitting in her mom's bedroom, typing on her mother's lap-top computer with the intention of downloading the latest song that her friends are singing in school. She goes onto a peer to peer website and, in just a few seconds, several "hits" are received. She double-clicks on the first one, and in an instant, she downloads a virus that automatically downloads child pornography onto her computer that saves it as a permanent screensaver! This is a true story that was told to me by a caller on a radio show.

Here's another true story. A very intelligent dad, who is a former judge with an M. Div and a Juris Doctorate shared with me that his computer is down. I asked him why and he sheepishly said his kids had been playing on a site called KaZaa and a virus ate his hard drive. I thought he would faint when I informed him that the site contains often mislabeled porn. He kept saying, "I had no idea."

David Wilson, professor of criminology at the University of Central England in Birmingham, said: "Peer-to-peer facilitates the most extreme, aggressive and reprehensible types of behavior that the Internet will allow." (Tuesday November 4, 2003—The Guardian)

I would like to close my testimony by stating, we know from volumes of research that people who view child pornography often eventually act out their fantasies and molest or rape children. We also know that pedophiles usually share graphic porn with young children to break down their modesty and resistance.

New technology is so valuable to us as a country, but with it comes new challenges and responsibilities. I always tell parents that they must be the first line of defense and remain vigilant against all threats including dangers on the Internet. The family computer should be kept in the family room where parents can intervene if a problem occurs. Computers in homes, schools and libraries need to utilize filters to block graphic images. Children should be kept from chat rooms and instant messaging without direct parental supervision.

The companies profiting from the technology must also share in the responsibility. Just as the ISPs are working to tighten its content and shield kids so must the peer to peer systems take responsibility. The FTC should use its authority to force companies to give parental warnings and to screen viewers of pornography by requiring ID. We should also make illegal the free teasers that pornographers use to lure in viewers without ID

Last July our country was sickened by an AP story on the indictment of twelve Suffolk, NY residents on charges of child pornography. Apparently the pedophiles had been using Kazaa, a peer to peer file sharing program, as a means to pass around vile images of their own or someone else's rape of toddlers. Congress needs to answer with passage of H.R. 2885, "The Protecting Children from Peer to Peer Pornography Act" or P4 bill by Joe Pitts (R-PA). Thank you for allowing me to testify before you today.

Mr. STEARNS. I thank you.

Mr. Lafferty, you think you're all set? Welcome you for your opening statement.

**STATEMENT OF MARTIN C. LAFFERTY**

Mr. LAFFERTY. The DCIA is a trade group founded last July to commercially develop peer-to-peer file sharing for legitimate purposes. Our charter calls for balanced membership among content providers, software suppliers and platform companies. We currently have 15 members and are actively expanding.

The internet is of great value as a productivity tool, enabling low cost conductivity, fast data transfers and a highly efficient marketplace. But it is neutral as whether such commerce may be legal or not.

Peer-to-peer file sharing, one of the internet's newest advances, replaces costly and relatively slow centralized servers with client software search engines that access other PCs for both discovery and delivery of content. The entertainment industries have generally failed to stay current with technology. And in the absence of authorized mainstream content, the internet so far as attracted a disproportionate amount of pornography. Dissemination of criminally obscene content, as well as legal adult material is facilitated by internet browsers, search engines, e-mail, instant messaging, websites, peer-to-peer software, chat rooms and news groups used regularly by tens of millions of U.S. citizens.

And with an increasingly decentralized internet, users themselves are frequently the sources of content and distribution. Porn websites have increased by 17 times since the year 2000, from 88,000 to 1,600,000 today. Thirty-four million Americans visit them monthly. But reports of peer-to-peer child pornography are down. From 2 percent in 2002 to 1.4 percent in 2003 with the vast majority of the remaining 98 percent coming from websites and chat rooms. And unlike websites, there is no commercial child pornography on peer-to-peer.

To demonstrate, leading file sharing software suppliers provide tools enabling parents to protect their children to exposure to undesirable content. Users can choose options to block adult content which is a default setting, add more key words to be blocked, pre-

vent all video and images from being downloaded and password protect their filter settings.

Use of these tools and monitoring of use by parents must remain the primary means protecting children. The peer-to-peer family filters set at the maximum levels, no files retrieved on searches for terms like Britney, Pokeyman or Olson Twins will contain pornography or child pornography. by contrast, MSN will return nearly 9,000 Olson Twins porn results; Google, some 820,000 Pokeyman porn results; and Yahoo, 1,260,000 for Britney porn.

Peer-to-peer companies have also worked proactively with law enforcement to prosecute criminals, abusers of their technology and on deterrence and education to further combat child pornography. Companies distributing file sharing software have responded to other issues identified by Congress with steady improvements. Examples include the integration of powerful anti-virus software and the implementation of default settings to prevent inadvertent sharing of private data.

The DCIA is now working with the FTC and others to address spyware. Leading peer-to-peer companies certify that their programs are spyware free. They offer consumers a choice of paid or ad supported versions. Their targeted ads collect no personally identifiable information and up to 40 times more efficient than traditional online ads.

But the real obstacle to realizing the potential of file sharing is the refusal of major labels and movie studios to license their content for legitimate paid distribution by peer-to-peer and it is this which deserves to be examined by Congress. At 50 million licensed files per month, DCIA members alone are now the web's largest legal distributors of copyrighted music, movies and games. This is accomplished through agreements with small, independent suppliers while the majors continue their boycott.

The entertainment industries lobby Congress with claims that file sharing is perilous to children. At the same time, these entities intentionally bombard them with shameful material. But it cannot be supposed that major labels have taken on partner and substance abuse, child abandonment, robbery, date rape or homicide as social missions. The entertainment industries' campaign to destroy peer-to-peer companies and to strangle file sharing technology is based on the assertion that they are suffering great economic harm through copyright infringement by individuals and that is simply not true.

Their emphasis on peer to peer pornography is unreflective of the much larger amount transmitted by e-mail and instant messaging, not to mention far greater risk of obscenity on websites and predatory dangerous in chat rooms and it is so dismissive of peer-to-peer suppliers' efforts to work with law enforcement and provide parental controls that takes on the character of a red herring.

Both copyright infringement and exposure of children to pornography are real problems and we condemn them, but how much more beneficial for all parties it would be if Congress adopted an alternative such as rights holders who wish to monetize digital distribution of their copyrighted works, must provide nondiscriminatory terms and conditions for all media.

Once the carrot of licensed content distribution can be offered, then the stick of enforcement focused where it should be on creators and disseminators of illegal material to be revisited.

Thank you. I'll be glad to answer your questions.

[The prepared statement of Martin C. Lafferty follows:]

PREPARED STATEMENT OF MARTIN C. LAFFERTY, CEO, DISTRIBUTED COMPUTING INDUSTRY ASSOCIATION (DCIA)

Chairman Stearns and Members of the Subcommittee, thank you for the opportunity to testify at this hearing. The Distributed Computing Industry Association (DCIA) is a trade organization, established in July 2003, for the purpose of commercially developing peer-to-peer file sharing and more advanced distributed computing applications for legitimate purposes. Our charter calls for representative membership among content providers, software suppliers, and platform companies. We currently have fifteen (15) members (listed alphabetically with links to their websites on the Join page at www.dcia.info) and are actively recruiting to expand our balanced and solutions-focused membership.

(1) The Internet is of immense value to society, particularly through its evolving and increasingly varied and decentralized usage as a tool for productivity, enabling exponentially faster and lower-cost means for connecting individuals globally, facilitating the exchange of all types of data, and creating a radically more efficient marketplace for commercial transactions. As with prior great communications inventions, Internet technology is neutral—facilitating communication without regard to whether content, or a transaction itself, may be deemed legal or illegal. Peer-to-peer file sharing, one of the newest advances of the Internet, is accomplished by client software search engines, returning queries from file directories, replacing costly and relatively slow centralized servers for both discovery and delivery of content, with an infinitely scalable number of participating PCs.

(2) Some content rights holders in the entertainment industries have failed to stay current with technology advancements, and not taken reasonable precautions to protect their products from unauthorized copying and online redistribution. They have confused the public by selectively enforcing their rights, and have boycotted prospective and willing new distributors rather than licensing them. In the absence of their broadly authorizing mainstream content online and labeling it to protect users from inadvertent exposure to inappropriate material, as in offline media, the Internet overall has attracted a disproportionate amount of pornographic content, and adequate safeguards to consumers are for the most part not yet being provided.

(3) Many computer users believe that the content they encounter on the Internet has been licensed and authorized as in other media that they routinely use such as television, radio, online subscription services, and various recording and playback devices. In Congressional hearings, computer users who have been sued by the record industry for alleged copyright infringement associated with online music redistribution, for example, have testified that they felt abused, prompting at least one US parent to sue the RIAA under RICO laws. Pornography on the Internet was initially limited by low bandwidth and limited sources. Those restrictions disappeared as modem speeds increased, broadband services proliferated, and pornography websites and chat-rooms multiplied. It has been challenging for Congress to balance consumer protection from undesired exposure with First Amendment rights issues. Credit-card routines intended to keep under-age users from accessing commercial pornography, for instance, have unfortunately proven easy to circumvent.

(4) More broadly, the dissemination of pornography, ranging from legal adult material to criminally obscene content, including the most pernicious category of child pornography, is facilitated online by such increasingly sophisticated electronic means as Internet browsers, search engines, e-mail, instant messaging, websites, peer-to-peer software, chat-rooms, and news groups, which technologies are now used regularly by tens of millions of US citizens.

(5) Such trafficking in pornography creates new challenges for content rights holders, computer manufacturers, software developers, and Internet service providers, to help protect minors from inadvertent exposure to such material online, and to educate the public, deter potential abusers, and enforce laws against dissemination of illegal material.

(6) In light of these considerations, responsible content providers and legitimate technology companies have an increasing opportunity to collaborate to protect consumers from inadvertent exposure to undesirable and illegal content, through appropriate and applicable technical solutions, business practices, and educational programs. All stakeholders should be encouraged to explore such measures in good

faith as well as adopting business models for legitimate content to be digitally distributed.

(7) With the increasingly decentralized topology of the Internet, users themselves, including consumers of pornography, now serve frequently as the sources of content being entered into distribution, as well as being the recipients of it. Therefore, unfortunately, it is not remarkable that pornography is being distributed through many online technologies. As this activity has grown, it has become more difficult to obtain accurate data as to exact quantities and the precise nature of such content. Nevertheless, the following studies and reports demonstrate salient facts regarding such pornography on the Internet:

(A) April 2004 reports from Websense, Nilesen/NetRatings, BigChampagne, and WebSpins indicate that pornography websites have increased seventeen-fold (17X) from eighty-eight thousand (88,000) in 2000 to nearly one-million six-hundred thousand (1,600,000) today; thirty-four million (34,000,000) people or about one-in-four US Internet users visit them monthly, and thirty-seven percent (37%) have visited a porn-site at work; approximately four and one-half percent (4.5%) of downloaded peer-to-peer content is pornographic images, while approximately nineteen and three-tenths of a percent (19.3%) is pornographic videos.

(B) A November 2003 supplemental report from the General Accounting Office (GAO) to the Senate Judiciary Committee stated that the risks of inadvertent exposure to pornographic content using peer-to-peer file-sharing software are no greater than those posed by other uses of the Internet (such as browsers, e-mail applications, instant messaging, websites, chat-rooms, news groups, or commercial search engines). Some 840 instances of reported child pornography were attributed to peer-to-peer software usage out of a 62,000 yearly total. 45,035 were on the Web, 12,043 were by e-mail, and 1,128 were on Usenet bulletin boards.

(C) According to the National Center for Missing and Exploited Children (NCMEC), reported child pornography on peer-to-peer was down from 2% in 2002 to 1.4% in 2003, with the vast majority of the remaining 98%+ coming from websites and chat-rooms.

(D) Further, as confirmed by DCIA member reports, unlike websites, there is no commercial child pornography distributed by means of peer-to-peer applications.

(8) Thus, while the use of file sharing software for the distribution of pornography is regrettable, it is less of a problem than activity in many other online environments. Finally, the leading file-sharing software suppliers provide tools enabling parents to protect their children from exposure to undesirable content. Users can choose options to block adult content, which is the default setting, add more keywords to be blocked, prevent all video and images from being downloaded, and password-protect their filter settings. While parental controls designed for search engines and other Internet applications, or distributed as stand-alone programs, may not automatically work with peer-to-peer software applications, the customized filtering solutions that have been incorporated in the leading file-sharing software programs are unexcelled in the levels of protection they provide and are setting the standard. Use of these tools and monitoring of use by parents and custodians must remain the primary protection of children from inappropriate Internet content.

(9) Beyond the provision of parental control tools, leading peer-to-peer software companies have also worked cooperatively and proactively with law enforcement agencies on programs to facilitate prosecution of abusers of their technology, who attempt to distribute criminally obscene content. It should soon become apparent to distributors of such material that sharing it via peer-to-peer public folders is the best way to expose themselves to identification and prosecution. Leading peer-to-peer software companies are also working voluntarily on deterrence and education programs to further combat child pornography before enforcement actions are necessary. The DCIA, for example, is focusing its resources on a collaborative program to enable peer-to-peer users to recognize, report, and remove criminally obscene content from their computers.

(10) While no amount of child pornography can be tolerated, the charge made by entertainment interests that peer-to-peer software exposes even children conducting unfiltered searches to a greater amount of pornography than those using an unfiltered Internet search engine is unsupported by evidence. Furthermore, in contradiction to these disingenuous allegations, using family filters included with leading peer-to-peer software applications set at the maximum level, in direct refutation of specific entertainment industry allegations, no files retrieved on searches for popular terms like “Britney”, “Pokemon”, and “Olsen Twins,” will contain pornography, child pornography, or child erotica. By contrast, searching on these same terms

using unfiltered search engines will yield many thousands of pornographic and criminally obscene results.

(11) Entertainment industry comparisons of relative growth of pornographic files are also misleading. Their cited peer-to-peer figures typically correspond to the period of greatest growth in the consumer adoption of peer-to-peer software and actually represent a more than fifty percent (50%) reduction in the complaint-to-user ratio. By contrast, websites, chat-rooms, news groups and bulletin boards, already well established and relatively mature, represented more than ninety-seven percent (97%) of reported incidents in this period. The record demonstrates that these issues have been and are being addressed, despite the greater challenges posed by a decentralized, user-generated file-sharing environment, resulting in a user experience comparable to, if not better than, that of surfing the Internet generally. While this concludes comments on the specific subject of this hearing, the following addresses other issues raised by the Subcommittee.

(12) The innovative companies developing and distributing publicly accessible file-sharing software have also responded to other issues identified by Congress and through self-regulatory processes by making steady improvements. Additional relevant examples of their commendable track record include the integration of strong anti-virus software with peer-to-peer file sharing applications, and the implementation of default settings and procedures to prevent inadvertent sharing of private or confidential data. Users can flexibly select the frequency of updating virus definitions; leading peer-to-peer companies promptly alert users of known attacks; and protected users help shield other users of file-sharing applications. With respect to safeguarding private information, current leading peer-to-peer software requires users to take multiple affirmative steps in order to share files that may include personal data. Peer-to-peer software suppliers have affirmed their commitment to further reduce risks and enhance both the safety and value of the user experience on behalf of their consumers and the public at large.

(13) The DCIA is currently addressing spyware/adware, in part by working with two DCIA member companies in the Center for Democracy & Technology (CDT) led Consumer Software Working Group (CSWG) since its inception. The DCIA also testified at the Federal Trade Commission's workshop in April 2004. At this event, it was made a matter of public record that leading peer-to-peer file-sharing suppliers, in addition to integrating powerful anti-virus software, now also certify that their programs are spyware-free. In addition, these suppliers offer consumers a choice of paid or ad-supported versions of their programs, with no pop-up ads appearing in the paid versions. Targeted advertising in the ad-supported versions collects no personally identifiable information, provides clear attribution as to its source, and is up to 40 times more efficient than traditional online advertising, meaning far fewer intrusions for users. Notifications are provided to consumers pre-installation, at download, and during operation; and the uninstallation of peer-to-peer programs, along with any associated advertising software, follows the same standard add/remove procedure as other legitimate applications. The DCIA readily acknowledges that more needs to be done to achieve its goal of establishing best practices in this area, and welcomes the opportunity to also coordinate with Congress on this issue.

(14) As noted earlier, however, the real obstacle to realization of the full potential of peer-to-peer technology is the refusal of key content owners to license their content for legitimate, paid distribution via peer-to-peer file sharing. In this regard, the DCIA commends the Subcommittee for scheduling a hearing on HR 107 "The Digital Media Consumers' Rights Act" on May 12, 2004, in contrast to the Judiciary IP Subcommittee's introduction and reporting in a single day, with no hearing, of HR 4077, a measure that could criminalize millions of young Americans, given its vague negligence standards, for merely storing digital music on a networked device. The entertainment industries' strategy is to combine their refusal to license content with their aggressive attempt to demonize peer-to-peer technology, in an attempt to crush what they erroneously view as a threat to their interests. This is the same time-dishonored strategy they tried in the futile fight against photocopiers, video recorders, and many other innovations that have brought great benefits both to consumers and to the companies that at first opposed them. And it is *this* which deserves to be the subject of Congressional investigation.

(15) DCIA members alone represent, with an average of 50 million licensed files now distributed monthly, the largest form of distribution of *legally* traded copyrighted music, movies, software, and video games on the Internet. This is accomplished primarily through agreements with small independent content suppliers, while the major studios and music labels continue their boycott of peer-to-peer. Nevertheless, licensed content distribution continues steadily to increase via peer-to-peer software programs. The challenges presented by digital content are indeed multifaceted, and no single response is sufficient. But among the different solutions

that have been tried by the major music and movie rights holders, the most glaring omission is the most obvious one—providing consumers with legitimate choices in each digital medium, including peer-to-peer.

(16) However, the continuing failure of the major labels and movie studios to license the peer-to-peer distribution channel exposes these users to potential lawsuits from the record industry for copyright infringement. This is the only unique threat that users of these applications face, and Congress should urge major labels and movie studios to swiftly license their content for all digital media, including peer-to-peer, in furtherance of the public interest.

(17) The full potential of peer-to-peer technology to benefit consumers has yet to be realized, and will not be achieved until content rights holders license their copyrighted works on a non-discriminatory basis for legitimate distribution by means of file-sharing applications. The ongoing boycott by major music labels and movie studios poses an increasingly serious threat, causing substantial damage to consumers, who are being harassed and threatened unnecessarily with lawsuits; to their shareholders, to whom they are denying a promising new revenue stream; and to content creators, particularly the independent labels and filmmakers seeking to monetize their copyrighted works using peer-to-peer distribution channels. The widespread availability of unprotected content from the majors severely disadvantages the independents from competing to sell their products using this most advanced and cost-effective distribution method.

(18) The companies that develop and distribute peer-to-peer file-sharing software have made energetic efforts to license content from the major labels and movies studios, but have been consistently rebuffed, in what may constitute a collusive refusal to deal. Related to this, a technical amendment to HR 1417, providing a blanket anti-trust exemption for music in all digital media, was passed without hearing, resulting in a thousand-fold windfall benefit to record labels.

(19) The current legitimate digital music marketplace is inadequate to properly serve consumers. Pricing at now licensed online music stores, for example, is maintained at artificially high levels so as not to compete with offline CD sales through an entrenched distribution infrastructure. Online store technology represents an older generation, less efficient centralized architecture. The quantity and quality of digital files made available for online sale are kept low so as not to be competitive with CD sales. Comparatively few users access these stores and fewer purchase files from them. The legitimate digital music marketplace needs to be expanded to encompass current and future technologies, including not only the latest Internet-based application, peer-to-peer file sharing, but also future technologies, with the requirement that music rights holders, and copyright holders generally, who wish to monetize their content in the digital realm, license it on non-discriminatory terms for all digital media.

(20) Returning to the subject of this hearing, the entertainment industries are lobbying Congress with claims that file sharing is perilous to children and that peer-to-peer companies, though they have no control over user actions, should be responsible for the content of files some users independently share. At the same time, these entities intentionally and continuously bombard impressionable children and youth with shameful material. Major labels peddle hate-filled and reprehensible lyrics condoning, even promoting, criminal conduct, from drug trafficking and matricide to rape and theft. By their actions, these companies demonstrate they are motivated by a determination to protect their revenues and not by any tenderness for the young. Their conduct goes beyond unclean hands to a pernicious business model that should be reviewed by Congress as part of its media indecency initiative. Can it be that to incentivize the creation of a wide range of responsible entertainment we must at the same time make wealthy those bloodless cynics who shamelessly trade children's innocence for money and who undermine values such as faithfulness, work, sacrifice, selflessness, tolerance and self-discipline? Is this what the framers of the Constitution had in mind when they authorized the creation of copyright laws?

(21) There can be no doubt that the ultimate motivation for such works is money. It cannot be supposed that any artist or corporate official has taken on partner abuse, child abandonment, robbery, date-rape, homicide, or revenge as social missions that they would pursue absent the lure of dollars. Yes, such expressions are protected under the First Amendment, but where is the policy that says we must also facilitate the enrichment of their creators and promoters by imposing draconian measures on the citizenry? While this last line of argument takes us beyond the parameters of this hearing, the astonishing hypocrisy of the entertainment industries in this regard had to be pointed out.

(22) A primary reason the DCIA has felt compelled to comment at such length is that the entertainment industries' ongoing campaign to destroy the peer-to-peer

software companies and to strangle file-sharing technology has gone largely unanswered. It is based upon the unproven assertion that labels and studios are suffering great economic damage through the copyright infringement of individual users. The DCIA's mission is to develop and promote the legitimate uses of P2P functionality, and to help foster business models that make partners, rather than litigants, of content owners, technology companies, Internet service providers, peer-to-peer software companies, and consumers.

(23) The entertainment industries' continuing emphasis on peer-to-peer pornography is unreflective of the much greater relative presence of pornography on the Web, and of the much greater ease of transmitting pornography via e-mail and instant messaging attachments, not to mention the far greater risks of criminally obscene content available on websites, and of predatory dangers in chat-rooms. And it is so dismissive of peer-to-peer providers' efforts to work with law enforcement and to incorporate parental control software into their products that it starts to take on the character of a red herring. The inaccurate pornography charge too, is one of the pillars of the entertainment companies' platform for destroying the nascent distributed computing industry, oblivious to the damage wrought by their own intentional and shameful role.

(24) Both copyright infringement and exposure of children to pornography are real problems, and we condemn them. However, we also encourage Congress to consider the possibility that the entertainment industries' ceaseless chant of piracy, and their unbalanced and diversionary claim of pornography, are not such issues as demand an inexorable tightening of the legislative screws on millions of Americans, young and old, by an angry Congress on behalf of unworthy supplicants. Instead, we commend to you the idea that these campaigns, on which so much money and so many words have been spent, are excuses that serve the purpose of shielding poor management from investor scrutiny, and of substituting for a lack of strategic business vision and for a lack of artistic creativity, and for an inability to learn from the lessons of the past regarding the development of earlier media distribution technologies.

(25) How much more beneficial and constructive it would be for the United States and all of its citizens, and for the entertainment companies themselves and their shareholders, if as the next step in development of the new and rapidly changing decentralized digital distribution marketplace, Congress were to adopt an alternative along these lines: "*To be effective on the date of initial publishing of a copyrighted work, any rights holder who wishes to monetize the digital redistribution of such work on the Internet and otherwise, shall be required to provide in advance terms and conditions on a non-discriminatory wholesale basis to all distributors, including software suppliers and individuals, who may wish to engage in such redistribution.*" Once the law has been modified in such a way to ensure that the "carrot" of legitimate licensed content redistribution can be supported given the realities of technical advancements now affecting the topology of the Internet itself, then the "stick" of enforcement could reasonably be revisited, with more appropriate requirements for commercial parties who may then be expected to bear increased responsibilities for protecting the new forms of commerce so enabled. These would logically include appropriate labeling and warnings for adult content, actions to combat criminally obscene content, and other measures to fully legitimize online entertainment distribution.

Thank you for the opportunity to provide this testimony. We would be pleased to answer your questions and arrange a peer-to-peer technology demonstration at your convenience.

Mr. STEARNS. I thank you. Well, I think we have a classic debate here between the P2P, peer-to-peer here saying that it's a neutral technology and has great worth and we're not sure that some of the solutions perhaps that have been offered in the Pitts Bill are practical, isn't that what you're saying, Mr. Lafferty? You're saying that the Pitts Bill is not something that you support?

Mr. LAFFERTY. Well, we've worked with——

Mr. STEARNS. Yes or no, would you support the passage of his bill?

Mr. LAFFERTY. We'd like to work with them on it more so. In its current form, we can't support it.

Mr. STEARNS. You could not support it in its current form.

Mr. LAFFERTY. I'd like to explain.

Mr. STEARNS. Let me ask you this, though, you can put filters on it, but can the filters actually look into the content of a file? I mean I can put the filters on all day long, but if I'm—if the server, the IP is—he can put a name and that name comes in and then bingo, you've got pornography, child pornography. So the filters really don't work in the sense that they can't detect what's actually the image or the graphics or what's inside. Isn't that true that the content can't be detected through a filter?

Mr. LAFFERTY. Correct. These are key word filters. The parents can add their own key words as they discover content that's problematic to block out both the title of the file and the metadata that goes to describe the file. So the best solution right now is for parents of young children to use the block all video and images mode where everything is blocked.

Mr. STEARNS. So all images would have to be blocked to make the filter work right.

Mr. LAFFERTY. Which it does have.

Mr. STEARNS. Mr. Dunkel, you at the University of Florida now had this peer-to-peer in all the dorms. The University of Florida has 46,000 students and you can imagine before you got involved with the program you had all this pornography and movies and everything going and you found it so disruptive, as you told me, that it slowed down the whole system because everybody was downloading all the time. So you put in your software and I guess the obvious question would be would the software that you use be effective for the family? Maybe you can talk about that you and your associate on how that would work for a family and should this be a software program that they can buy and how would it actually prevent the content and give a filter—how did you do it so that you just blocked all video, is that the way you did it?

Mr. BIRD. What we chose to do was we chose to prohibit the mass distribution of content from individual machines. We felt that that was an appropriate use.

Mr. STEARNS. What does that mean, the mass distribution of content?

Mr. BIRD. Well, many years ago, in fact, about seven years ago, we created policy that said we're not going to allow servers to run in our residence halls and that essentially means is at that time we were facing a problem of commercial abuse of our resources in the residence halls. So as an extension of that, we noticed that there was rampant abuse of these peer-to-peer applications for one person's ability to distribute content to millions of other folks. And what we found is that the connections are so significantly faster than your average home broadband user that actually residential users on college campuses have tremendous opportunity to distribute in a way that even your best home user cannot.

What we chose to do was we chose to stop the distribution of essentially all files by those mechanisms, so we stopped websites, we stopped peer-to-peer applications, we stopped a large number of things and redirected the residents to appropriate resources for their needs.

Mr. STEARNS. So you just put up a wall?

Mr. BIRD. We basically put up a wall, but that wall is very difficult to maintain without an application like this.

Mr. STEARNS. And I don't know if that would be a practical application. I guess it could be for a family if young children, but that wall also prevents peer-to-peer for music if a student wanted to download music or a video, for legitimate concerns.

Mr. BIRD. Correct. The one thing that we found is that the wall that we have in place at the University of Florida is not specific to ICARUS, so the application itself can be used in a variety of different ways. It's not specifically a block all or nothing sort of scenario. It could easily be customized for home use and in fact, the version that we're working on presently does just that.

Mr. STEARNS. That seems to me the key that if you had a software that's not either or that it could still have the nuance to allow legitimate—

Mr. BIRD. Correct.

Mr. STEARNS. I guess the real key would be to be able to actually survey the content. You could have a filter that says okay, based upon name, but once a name came up and allowed it in, it actually looked at the content. Now I don't know how you technologically, that's not available yet where you can actually survey the content of these downloaded programs.

Mr. BIRD. It would be possible to build a variety of databases that might cover certain file formats, for example, that's been done in the copyrighted music industry. Certain commercial companies have built databases that will detect the transmission of copyrighted materials explicitly, but it essentially is impossible to monitor and block explicitly on content because content can be compressed, it can be encrypted and there's no way to actually analyze that.

Mr. STEARNS. Well, my time has expired, but I would say to Mr. Allen, I guess a hopeful sign would be if the University of Florida can detect and prevent peer-to-peer in a negative way, and ISPs are required by law to report any child pornography on its sites, perhaps two of these processes could come together to help you, wouldn't you think?

Mr. ALLEN. Mr. Chairman, I think it would be enormously helpful and let me thank you and the Members of the Committee. The fact that Congress mandated in 1999 in the Protection of Children From Sexual Predators Act that ISPs have to report child pornography on their sites to law enforcement. Through our CyberTipline at the National Center has produced hundreds of prosecutions and arrests and is generating thousands of leads. So I think the combination of technology and we're very much in support of filters and other technologies. Ms. Nance pointed out most parents still don't use them. But I think it's a great tool. It's just not a panacea. Enforcement has to be a key element to the equation.

Mr. STEARNS. Thank you. My time has expired. Ranking Member?

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. Mr. Lafferty, a few moments ago you noted that you couldn't support the Pitts Bill in its current form and I wondered if you just take a minute to explain what legislation you could or what changes you feel need to be made.

Mr. LAFFERTY. We welcome the opportunity to work with Congressman Pitts' staff on those issues. A couple of points, one is that

that bill seemed to say in its subtitle, it singled out peer-to-peer, the subtitle was to ban peer-to-peer. So of course, that's a problem for us.

When we talked about the real intent of the bill which is to protect children, given that there's so much more of child pornography and obscene content on websites and chat rooms, we felt strongly that that bill should be broadened to cover other instances of child pornography and criminally obscene content on other parts of the internet. And there's some technical questions about the notion of a beacon which the bill contains. So we think the way to go is to continue on the path of developing more and more powerful family filters as we've been discussing this morning and apply it to the internet as a whole. And we would welcome the chance to work more on a bill to protect children from pornography on the internet.

Ms. SCHAKOWSKY. You also had a different interpretation of what was available on the internet. And that the Google searches that you were talking about produced a good deal of pornography. Was the filter in place when you did that? How come there's such a discrepancy between what Ms. Nance found and what you found, Mr. Lafferty?

Mr. LAFFERTY. The commercial search engines generally don't provide a filter, so it's a third party filter like the NetNanny that could be added as separate software, where as the P2Ps actually integrate a family filter into their software that downloads it into default position. I didn't do that search. I can't comment. We did the one that we did and we compared using the family filter integrated with Kazaa with just a straight search on Google, Yahoo and MSN and those were the results.

Ms. SCHAKOWSKY. Ms. Nance, you said that a filter was in place when you did the Cinderella search.

Ms. NANCE. It was in place and it was the adult filter that Kazaa provides, but I want to say even if parents were able to think of all the possible search terms that some person could possibly some twisted person could come up with to try to snare in kids, if I could think of all of those and I could passport it and I could put it on there, the only thing that happens is that the kid put in the password is a popup dialogue box that says would you like to disable the filter and it's a yes or no. Or, if you've got a savvy, curious 13-year-old that gets on there and it popups and says or he can't get into what he wants, all he has to do is redownload Kazaa or one of these sites and in two minutes he's back in business without any kind of filter at all.

Ms. SCHAKOWSKY. Mr. Catlett, you were suggesting all these really wonderful uses of the P2P network. What would happen to those if, as written, the legislation were to pass?

Mr. CATLETT. I'm frankly not sure that the applications that I showed would be impacted by this bill. I'm not a lawmaker, and so I may not be reading it correctly, but so I'm not sure my applications that I showed would be impacted, but I think it's possible depending on the implementation of the bill that—I'll give you an example, the bill describes peer-to-peer software in a way that, as I said, includes instant messaging and other things on my computer.

It has an exclusion for operating system software like the McIntosh operating system I run here or Windows on this machine,

as I read it. And that would make me a little bit nervous because if we exempt the operating system then a large company that provides an operating system could build new technology into their operating system under a different set of rules than a small company developing software whether it's peer-to-peer or something else.

I look at that bill and I read the bill and I just absolutely am thrilled that you are taking this one and I see some very good ideas in there and I think with the turn of a crank, with collaboration with some software companies that it could be a reasonably good bill.

Ms. SCHAKOWSKY. So that even those of you who oppose the—who have some problems anyway with the legislation as written, feel that technologically we can address adequately the situation of children getting access to this pornography?

Mr. CATLETT. If I can answer, I think one of the things that we're seeing here is peer-to-peer technology is very new compared to web searches and it doesn't have the jump. Web searches have been around for 10 years. Ten years ago when my 16-year-old daughter was in second grade I had her whole classroom come in to where I worked at the time at the University of Illinois and I wanted to use our classroom there was internet connected to do a scavenger hunt to show the kids the internet. The night before I typed into one of the search sites "Barbie" and I forgot to put the E on the end and I got a different kind of Barbie that I thought I was going to get. So I worked the whole curriculum to constrict what the kids were able to search for the next day when they did that.

I wouldn't have to do that today the way I did before, but I would if I were using peer-to-peer technology say a year ago. I'm not sure what's happening lately with peer-to-peer technology, but it does change a lot in a short amount of time.

I also did extensive research last week in that I asked my 16-year-old how this works for her. I said how often is it that you are using Kazaa and she like to downtown television shows that she missed and things like that. How often do you get inappropriate content when you search? She said well, at first I saw some inappropriate things maybe last year, but I've built up my filters to the point where I never get inappropriate things any more with one exception, she said, there was one time she downloaded what was supposed to be a sitcom, a Friends show or something like that and it was actually something else and she figured out from the title when the movie started that it wasn't the kind of the thing—so it's not full proof, but it's come a long way and that's what I said earlier. Harnessing the innovation and technology in the software field to address this problem I think is really a good approach. And also the idea—so my 8-year-old can pick up a snack and he says Dad, this has a lot of fat in it because he understands these simple labels. What I wish my 8-year-old could download software and say hey, Dad, I think this software has some privacy issues, maybe we shouldn't install it. So simple labels and notification would be tremendous and not just for this software, but all software.

Ms. SCHAKOWSKY. Thank you.

Mr. STEARNS. The gentlelady's time has expired. The gentleman from Pennsylvania, Mr. Pitts.

Mr. PITTS. Thank you, Mr. Chairman, thank you to the witnesses for your testimony.

Mr. Catlett, first of all, I appreciate your comments on our Bill, H.R. 2885, in your written testimony. In your opinion is it technologically possible to develop a do not install beacon?

Mr. CATLETT. I think it is. I read that part of the bill and I was intrigued by that idea. Depending on how it's implemented, it just simply has an impact on the software engineering costs and support costs of companies that are doing software and operating systems. And so is it technically possible, certainly. Depending on how it's implemented, it could be either very easy or it could be very onerous for software developers.

Mr. PITTS. You expressed concerns about how peer-to-peer is defined. Would you be able to provide us in writing your recommended revisions to the definition? I'd like to work with you to ensure that the definition is not so broad as to have unintended consequences for legitimate peer-to-peer uses.

Mr. CATLETT. Certainly, I'd be happy to try to look at that and even engage some of my colleagues. One of the things about that is it's very difficult to precisely define software, but I'm not if it's impossible or not, but it's very difficult. I made my comments because I would like to help, yes.

Mr. PITTS. Thank you. Mr. Lafferty, in your testimony you mentioned the music industry, they should also be held accountable. I know that the music industry has to go before the FTC for the approval on their content. Do peer-to-peer distributors go before the FTC for the content they distribute?

Mr. LAFFERTY. The peer-to-peer software does not distribute content. It's a technology. The content is put there by the consumers. We appeared on the FTC panel on spyware. We're working closely with the FTC on that issue and expect to continue to work on that to establish industry best practices that will be acceptable to society.

Mr. PITTS. Now you mention in your written testimony that there 840 instances of reported child pornography that were attributed to peer-to-peer software usage. Have your member groups acted proactively to make sure pornographic material is not on their network? If so, what steps have you taken to proactively help law enforcement?

Mr. LAFFERTY. We've been working with the FBI for a number of months and not to step on anything, covert operations that can't be disclosed, it should be apparent to all that P2P is the dumbest place to put illegal materials like standing in the middle of a town square and saying look at me, I have something illegal. You will get caught and quickly and prosecuted. So we're very pleased with that aspect of it.

We're also working with them on deterrence and education programs to help users recognize, remove and report criminally obscene content and using new technology that's not the keyword filter, but a collaborative filtering approach to be able to cleanse the P2P services from objectionable content with the users engaged in doing so.

Mr. PITTS. You mentioned users again choose options to block adult content which is the default setting. How does the adult filter

work? The filter works by blocking search terms, right, not actual files based on content. And, what search terms trigger the adult filter on Kazaa?

Mr. LAFFERTY. And it is a bit of a blunt instrument at this point. Yes, it's a very new industry. We're less than 10 months old, not to make excuses, because no amount of child pornography is acceptable, but it works in two modes. You can enter key words that are in the title of the file, put there by the individual who distributed that file and the metadata that describes the file. So if there are adult words in that, it will block it out.

The second mode which is what I recommend for parents with young children, it blocks all images, blocks all video. So really two modes, blocking words up to a certain point and then stronger mode, maximum level to block all video and images to fully protect children.

Mr. PITTS. If you search by a term that does not trigger the adult filter, such as baseball. Does the filter block pornographic material?

Mr. LAFFERTY. Only if the metadata had some reference in it that would trigger that adult level or if the parent had added the word baseball to block that. Again, it's a keyword filter. It has limitations. I think it's been developed as far as it can be to be as effective as it is, which is why the separate higher level of blocking all video images is also provided.

Mr. PITTS. Now if you use the maximum level, I think you used that term which means images and video filter set, you can't download movies or concert videos or pictures of Barry Bonds hitting his 600th home run, right?

Mr. LAFFERTY. Correct.

Mr. PITTS. What is a parent or child for that matter, doesn't want to block all images. They want maybe a G-rated movie. Is the adult filter the only other way to block adult content?

Mr. LAFFERTY. Currently, that's correct. We're working on—we're not resting on any laurels here by any means and member firms are working on collaborative filtering which I mentioned which is a new technology that allows users to tag a file as being objectionable or criminally obscene and then it will be pushed out of distribution on a particular P2P software application. That's new and it's coming along. In addition, working with the FBI on deterrence popups to warn users and on education programs, further education programs to help consumers recognize, report and remove content.

Again, it's a new technology and certainly we're pleased to see that the incidents dropped from 2 percent of all of the reports to 1.4 percent last year, but we won't be satisfied until it's zero. It's just a continuing effort to fight, to combat child pornography and get it off of these services.

Mr. PITTS. My time is up. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. The gentleman from Ohio, Mr. Strickland.

Mr. STRICKLAND. Thank you, Mr. Chairman, and I want to thank the witnesses. Mr. Lafferty, if I understood your answer correctly to Mr. Pitts, you are responsible for the peer-to-peer technology. You are not responsible for materials that may be made accessible or available through the use of that technology. Is that correct?

Mr. LAFFERTY. We're a trade association, but answering for my members who are peer-to-peer software suppliers, speaking for them, that's correct. They provide the software and then 99 percent of the content is put there by users, put in a shared folder and shared with other users.

Mr. STRICKLAND. So you accept no responsibility for whatever content may be made available through the use of your technology? Is that a correct statement?

Mr. LAFFERTY. I wouldn't, no. There's a difference between knowledge and control of what the content is and providing parental tools to protect children. There are warnings, clear, conspicuous warnings about copyright infringement. There are any number of things being done to try to have this software be implemented for proper, legal uses, legitimate uses. That's what we're dedicated on doing.

Mr. STRICKLAND. Excuse me for interrupting you. I didn't intend to do that. You don't feel though that you should be held liable for illegal materials. I'm talking about child porn, specifically, that would be made available to children through the use of your technology. It's not a trick question. I'm just trying to discern what your position is.

Mr. LAFFERTY. Not to answer a question with a question, but it's—should Microsoft Windows Outlook be accountable for every single e-mail that all of its hundreds of millions of users can sort every day. The nature of the software is that individuals can put whatever they want on there and that's the problem we're having with the music industry that popular music is ripped and put online with no copy protection, no upload protection and it's there.

Mr. STRICKLAND. That brings me a question that I have for Mr. Dunkel.

Mr. Dunkel, you talked about the University of Florida's student body overwhelming downloading music and movies before you changed your policy. And I know we're here to talk about child pornography, but I think we cannot talk about this technology without bringing up another relevant matter which involves honesty and legality and all of that. And that has to do with copyright protections. I would be interested in hearing a little more, if you could tell me, what you at the University of Florida are doing in regard to your computer policy and steps you may be taking to educate students regarding the morality or legality of their behavior regarding copyright laws.

Mr. DUNKEL. Certainly. When ICARUS was originally turned on to date which is less than one year, we had discovered 3,700 first time violators. So these were students who were using their desktop knowingly or unknowingly as a server with music, video or images and once we identify a student so Mr. Strickland, we've identified your computer and whether you knew it or not, you had a file server program working on your computer, we would then terminate you from the internet. You would still have access to the University of Florida, so you'd have access to your courses and teachers and so forth, but not the greater internet. We would direct you to a website within our operation and it would take you through educational information to identify why what you're doing is not within our acceptable use policy, what you need to do and walk you

through the steps to take care of that. We would then time you out for 30 minutes. So you've had a first time violation. You have 30 minutes now that you're no longer on the internet. If we find you violating that a second time, you go through the same steps and you're timed out for five days. A third time, and you go through the University of Florida's Judicial Affairs process. So a record then, in Judicial Affairs is maintained by the University and a sanction is applied accordingly.

For most students, those 3,700 first time students, that would be the only time they ever hear of that. Three hundred fifty were second time violators and only 32 were third time violators and that included students who had viruses and worms hosted on their computers and they wouldn't take the steps to clean their computers. So we also deal with viruses and worms going through that program.

Mr. STRICKLAND. Let me congratulate you. It sounds like you've taken appropriate action to deal with what I consider a very legitimate problem.

If I could ask any other member of the panel, do you think that there's any responsibility on the part of those who make this technology available to also provide some kind of educational component to the user regarding what is and is not legal and appropriate in terms of copyright infringements?

Mr. LAFFERTY. We clearly think there is and we're working with our members and glad to work with Congress, the FTC and others to do that, do exactly that.

Mr. ALLEN. Yes.

Mr. DUNKEL. I would add just a further word that clearly the University of Florida as any other institution of higher education is in the business of educating students. We have to do that actively. We have to do that passively, so whether we're handing a brochure out or placing a sticker on their dataport or doing something on line, clearly, we have a responsibility to educate.

Mr. STRICKLAND. Thank you. Thank you, Mr. Chairman. My time has expired.

Mr. STEARNS. I thank the gentleman. Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman. I'm glad I had a chance to make it up here after my—the other hearing we had.

Let me ask—all of you are really tech savvy and understand what's out there. Let me ask a question to each one of you.

Is there a spot on the worldwide web where a parent can direct their children to go that is safe, that's reviewed, that does not allow peer-to-peer, would not allow spyware applications and is safe by the Federal definition, not harmful to minors under the age of 13?

Mr. Catlett, do you know of a place like that?

Mr. CATLETT. Well——

Mr. SHIMKUS. Basically, yes or no. Is there a site right now where parents can go for kids under the age of 13 to search for information that has no hyperlinks, in essence, no internet messaging, no chat rooms available?

Mr. CATLETT. I think you could set up a web browser so that it would——

Mr. SHIMKUS. The question is is there a site now, do you know?

Mr. CATLETT. Sure.

Mr. SHIMKUS. Do you know the name?

Mr. CATLETT. I would guess somewhere like I'll say lego.com wouldn't have any links off the site, but I couldn't verify that.

Mr. SHIMKUS. I would doubt that.

Mr. CATLETT. It may have links off the site.

Mr. SHIMKUS. It sure does. They all do. Let's just go down, Mr. Lafferty?

Mr. LAFFERTY. I am encouraged by KidsOnline which is a service of AmericaOnline, a subsidiary of AOL and we would like to have such a site using the P2P technology with the filter fully engaged, a kids Kazaa, which is completely safe and where the content is absolutely locked and——

Mr. SHIMKUS. You failed the test too. Mr. Dunkel?

Mr. DUNKEL. Our work does not venture in that area. I could not answer that question.

Mr. SHIMKUS. You should know them and we're going to educate you in a minute. Members usually don't educate.

Mr. Bird?

Mr. BIRD. I'm not aware of any technology like that.

Mr. SHIMKUS. Mr. Allen?

Mr. ALLEN. No.

Mr. SHIMKUS. Ms. Nance?

Ms. NANCE. There is no place I can turn my back on my children and allow them alone on the computer.

Mr. SHIMKUS. The answer there is a site, enacted in the law, signed by the President, 18 months ago. It's interesting that we have competing hearings today because we just came from the hearing. Kids.us. Safe site for kids on the internet. Doesn't allow peer-to-peer. Doesn't allow instant messaging. No hyperlinks. Information-based only. It's positive, voluntary and it's a site where we need help in getting people who want to provide safe information for kids. So pro-family organizations and groups ought to be hounding the private sector and the public sector to get up on the site. We have 13 active sites. They go from the smithsonian.kids.us, abckids.us. We have—in essence, there's 13 in total.

And what we are fighting is the chicken and the egg battle. NewStar manages the site. They have, I think, kids.net oversees the site. NTIA can pull down the site if there's anything that sneaks on that is inappropriate. Part of the job that I'm doing, as part of the author, along with Chairman Upton and Chairman Markey, Ranking Member Markey and then Ranking Member Dingell and Chairman Tauzin at the time when we passed this legislation is when you pass legislation you just can't let it go, I mean if you really want it to be successful. So I use the bully pulpit. I'm allowed to do that and that's what I'm doing now.

When we had the pornography hearings on the Super Bowl I looked at the network guys and I said how come you don't have a .kids site, a kids.us site? Guess who is now up, abckids.us.

So my plea is—the University of Florida ought to have one. If you want to educate children about the great aspects of the University of Florida in a safe arena for kids, so that maybe one day they may want to be a Gator, you ought to be there and so this is—I know you're here to educate us. There's serious problems.

In the hearing today I asked the question when I ended up and it was a very good hearing because it's the difference. Here we're trying to react to problems. We have a safe site now for kids and we're not promoting it. No spyware. You can't put spyware on a kid who is on the kids.us site. No peer-to-peer, information-based only and is reviewed by both the government and private sector contracted agency with ability to pull the plug.

So I'm using the bully pulpit. Thank you for being here. Spread the word.

Mr. Chairman, I yield back my time.

Mr. STEARNS. Gentlemen, we have your site right up on the screen to help you promote the site that your legislation originated and that you support and we're a strong advocate and the President signed your legislation and I thank you for your comments.

Gentlelady, Ms. McCarthy?

Ms. MCCARTHY. Thank you, Mr. Chairman. I thank the Panel and apologize for being late to your testimony. I had another full committee and subcommittee simultaneously.

But I am intrigued by the thought that there might be wisdom on other legislative alternatives that we could employ to address this, not only the unauthorized download of copyrighted information which is an infringement and punishable, but also to require porn sites to enforce laws or be terminated. And the RIAA recently brought lawsuits against university students for copyright infringement.

I wondered if any of you, particularly, Mr. Dunkel and Mr. Bird from the University, I'm very impressed with your effort. I wonder what the effect on students it might have potentially or have had with regard to the private sector weighing in with consequences just as you have chosen as an administration and a university and whether that is something that we should be looking at as a legislative alternative, the encouraging of such partnerships and such efforts, and what role the Federal Trade Commission could have or what more power they would need to be an effective partner in such an alternative. I would just welcome your thoughts.

Mr. Lafferty, you're welcome to weigh in.

Mr. DUNKEL. Certainly, I could share with you that prior to last summer, there are various agencies that would send out notice to educational institutions that a particular user is violating a copyright law and they would send out a DMCA violation letter. So a digital millennial copyright act violation letter. It would say Ms. McCarthy at this certain port and so forth, you're violating a certain part of the copyright law.

When we deployed ICARUS, prior to deploying ICARUS, our institution was receiving approximately about 60 or 70 of those per month. When we deployed ICARUS, we have not received one since that time. So I think we've worked very effectively with industry in helping to educate the residents and the program seems to be working well.

Ms. MCCARTHY. Any other ideas from any panelists on what other legislative alternatives we should be pursuing with the private sector and government regulatory bodies?

Ms. NANCE. I would just suggest, you know, there are probably things within Mr. Pitts' bill that we could all agree on like perhaps

parental warnings. I mean they're willing to put up parental warning for copyright infringement, why not pornography?

Very simply things that can just alert parents to what is happening. I would urge people to sit and talk to Mr. Pitts and for all of us to come together on the areas that we can agree on and to go forward because it's a serious problem.

Ms. MCCARTHY. Thank you very much, Ms. Nance.

Mr. LAFFERTY. You brought up the copyright issue. We have helped convincing the major labels and large movie studios to embrace this new technology and begin licensing their content for legitimate distribution so it can commercially develop. I mean the only unique threat that users have on P2P now, given all the other threats of other aspects of the internet is an RIAA lawsuit and the notion of bludgeoning your customers and trying to terrorize consumers is the wrong approach.

We need to have them legitimately license their content for pay distribution. We'd love to be working with the RIAA members on a program for this fall for college, to provide college students with a way to purchase songs, legally, at attractive prices and that would be a terrific solution. It will be a revenue generator on a voluntary basis, not some kind of a tax on students that the university has to put in place and not a cost, an expansion of commerce.

Ms. MCCARTHY. Thank you and I quite agree. My concern remains that a young person would be going up on a peer-to-peer situation to download a Britney Spears song and while there, is confronted with pornographic pictures of a Britney Spears of some sort and how to separate those two. But I don't know that that's a legislative solution as much as it is just the industry and others working together as they have been doing to try to address it and I thank you, Mr. Chairman.

Mr. STEARNS. Thank you. The gentleman from New Jersey, Mr. Ferguson.

Mr. FERGUSON. Thank you, Mr. Chairman. I have a couple of questions for Mr. Lafferty.

Mr. Lafferty, it's common for one of these services and I begin by saying that I'm not familiar with Kazaa. I've never used it, so I'm a little bit ignorant on the actual use of some of these and peer-to-peer technology as well, but frequently, I would imagine for some of the folks that you represent and I know for some of these services there are these end user license agreements and they say, one of them that I saw says that you state that they do not allow their users to distribute obscene or illegal material to other users of the product. That's pretty common, I would imagine.

Mr. LAFFERTY. Correct.

Mr. FERGUSON. How is that enforced? It's obviously not true. There are obscene materials being distributed from one user to another. How is that agreement enforced? It sounds hollow to me.

Mr. LAFFERTY. The way to enforce it is working with the FBI, as we are, on these covert operations to identify, capture egregious users who are inserting criminally obscene content into the system in which case they'll be terminated because they're in violation of the agreement, but it's, as I mentioned to Congressman Strickland, the sheer volume of content, think of if you had to deal with Windows Outlook on all the e-mails being written every day and some-

how have knowledge and control of that, probably Microsoft would go into bankruptcy trying to do that. It's that type of issue. So when we see a problem work with law enforcement, identify it, prosecute the abusers and terminate them.

Mr. FERGUSON. How many folks have been terminated?

Mr. LAFFERTY. I can't comment on that because it's private—it hasn't been announced yet.

Mr. ALLEN. Could I comment?

Mr. FERGUSON. Could I ask, have any? Is that private?

Mr. LAFFERTY. So far the number of busts, prosecutions have been not great, but that's going to change and I think you soon will see that P2P is the dumbest place to try to disseminate criminally obscene content.

Mr. FERGUSON. Why is the bust rate, as you call it, why has it not been very good?

Mr. LAFFERTY. I think we're getting into some confidential—we'd like to talk about it privately with the FBI and not public.

Mr. FERGUSON. By your own description, the monitoring of this has not been particularly good, is that a fair characterization?

Mr. LAFFERTY. I think law enforcement thinks that perpetrators of illegal content on P2P, it's like—in their words, it's like shooting fish in a barrel.

Mr. FERGUSON. But what has the industry done to monitor itself?

What have the companies done to monitor—if—what does the FBI do to monitor these things? They get people to start surfing the net and being users. Can't companies do that as well? If the company has an agreement that says you're not allowed to do this, doesn't the company have some responsibility to monitor itself?

Mr. LAFFERTY. Sure.

Mr. FERGUSON. And do the companies do it at all?

Mr. LAFFERTY. The companies are most familiar with the technology and see the scale of the issue and so they attack it through other technology means such as the family filters which have come to a point of blocking all video and images.

Mr. FERGUSON. Forgive me, my time is short. The filters tend to be useless, don't they? I mean can't kids go in and can't you just download Kazaa again if your parents have put a filter on it? Can't you just go and download it again and get around the filter?

Mr. LAFFERTY. That's really an operating system, a browser issue.

Mr. FERGUSON. But the question is doesn't that render the filter useless?

Mr. LAFFERTY. Once the parents put the password in it locks that particular setting and you need to know the password to be able to break that setting.

Mr. FERGUSON. Can children get around these settings?

Mr. LAFFERTY. There's always going to be hackers——

Mr. FERGUSON. I'm talking about a 12-year-old kid?

Mr. LAFFERTY. Unless they find out the password, it works.

Mr. FERGUSON. But do the companies feel like their responsibility has been met simply by putting filters on that can be hacked through?

Mr. LAFFERTY. Absolutely not. This is a moving target. We're not going to rest until we've really defeated child pornography and

cleanse these networks. It's abhorrent and horrendous. So that's why other steps are being taken and deterrence, education, additional forms of filtering that are more sophisticated and the work continues. It's a very new industry. It's less than a year old. It's 10 months old.

Mr. FERGUSON. I appreciate that. And as you can tell and as I've said I'm not familiar with it, partly because it is so new.

Mr. LAFFERTY. What's happened is the consumer adoption rate has been fantastic. This has taken everyone on the content side of the table and the technology side of the table by surprise. It's taken our breath away and we're playing catch up to civilize it and to do the right thing.

Mr. FERGUSON. Let me just close since my time has ended, let me just close by urging you to work with your companies to take a more active role in monitoring themselves to help the FBI. I know you're working with law enforcement to do that. But if law enforcement can do that, the private sector has a responsibility here too and we're talking about legislation now and you've said that you can't support the legislation as it's currently written.

I don't speak only for myself. There are a lot of Members on both sides of the aisle in this body and certainly on this committee who are very concerned about this issue, feel that the industry has a real responsibility to continue to monitor itself, to do a better job of monitoring itself and it's our hope that you can continue to make progress on that and working with law enforcement because legislation is coming and if you don't like the legislation you've got to be willing to either work with us to make that legislation better and/or make it so that legislation is not necessary by doing the work yourself. If, in fat, you don't like the legislation that we're considering, you can help that. You can change that. The industry can do it itself and I would urge you to work with your members and the folks that you represent to do that.

Thank you, Mr. Chairman.

Mr. ALLEN. Mr. Chairman, could I comment, just very briefly?

Mr. STEARNS. Absolutely, sure. Go ahead.

Mr. ALLEN. I think Mr. Ferguson's point is incredibly important because this has not been like shooting fish in a barrel. Working these cases on P2P has been very difficult and it's very important and encouraging that this industry has stepped up in the last few months and is working with law enforcement, but the reality is people are fleeing, those predators who prey upon children and use child pornography are fleeing websites because of the increasing presence of enforcement. The ISPs now have an obligation to report child pornography on their sites. What we have to do to preserve the integrity and the potential of peer-to-peer and distributed computing is to make sure that it is not allowed to become a sanctuary for those who are seeking ways to operate in anonymity and violate and avoid the law. I think the steps they've taken are really important, but your message is one that the whole industry needs to hear loud and clear.

Mr. STEARNS. I thank the gentleman. Mr. Allen, just following up on that, do you think that—would you advocate that the peer-to-peer companies have to register with the Federal Trade Commission?

Mr. ALLEN. I think that's really beyond our expertise. The one thing that I think is really important and in the early days of the internet, the ISP community was concerned as well——

Mr. STEARNS. You advocate, you support the idea of the ISPs, have been mandated by Congress to report pornography and child pornography. Do you support that kind of idea for the peer-to-peer?

Mr. ALLEN. I think it's an excellent model that ought to be examined.

Mr. STEARNS. Well, Mr. Lafferty, I think you've heard sort of Mr. Ferguson's comments and I think everybody in this room has agreed in the goals of this subcommittee is to protect our children from pornography, child pornography. How we do it, whether we do it through Federal legislation or we do it through best practices, how many companies are there in the peer-to-peer organization now that you have?

Mr. LAFFERTY. We have 15 members and about 5 of them are in the peer-to-peer space. Five are content, five are service support.

Mr. STEARNS. How many do you think there are in the United States peer-to-peer?

Mr. LAFFERTY. Internet is global, so I can't—120 known peer-to-peer software service——

Mr. STEARNS. And that's another point I point out to my Members, cross-border fraud is very prevalent and this is a global market, so you have companies outside of the United States. It's very difficult. We passed a cross-border fraud and deception out of this committee at the request of the Federal Trade Commission. It's gone to the House. We don't have it out of the Senate. We'd like to pass that bill which would give the Federal Trade Commission reciprocity with other nations where we could actually go after those companies, bad actors. But it is all going to come down, I think as Mr. Ferguson has pointed out is whether your association is going to have a best practice, have a standard and actually work hard to make sure that the peer-to-peer technology is used in a useful way and we don't have the bad actors, but I think as you can see, we're so strong about this issue, all of us having children, that we're willing to consider legislation.

And Mr. Catlett, I'd appreciate if you would talk to Mr. Pitts and perhaps you can suggest things that would make it more feasible for it.

Is there anything in concluding? Ms. Nance, anything that—Mr. Allen, anything anyone would like to say before we close?

Ms. NANCE. Thank you again for convening this hearing and yes, I just want to agree with your last point. I think it absolutely—they should be obligated to report back to the DOJ any incidents they find of obscenity or pornography, and I just think that's the minimum they can do to help our families. So thank you.

Mr. FERGUSON. Mr. Chairman, can I just add one thing? I just want to thank Penny Nance, too, for the work she's done. She's done an enormous amount of work, pro family work for a number of years here on the Hill and around the country and starting this organization, she speaks for so many moms and dads and folks across this country who are working so hard, concerned about their kids, worried about what they're seeing on the internet. Our kids, as I say, are not old enough for using the internet yet, but they

will and it's coming. It's—there are certain things we can do on the legislative side, but as we know, there are certain things that need to be done by moms and dads and groups and associations of families who will speak up for people around the country who frankly sometimes feel like they don't have quite that voice that they want. We try to give them that voice through our representation, but there are organizations like hers which are doing a great job and I thank her for that as well.

Mr. STEARNS. Any other comments before we close? Mr. Pitts, anything?

Mr. PITTS. I'll just second those comments. Thank you very much, Mr. Chairman.

Mr. STEARNS. Thank you very much for your patience during this hearing and the subcommittee is adjourned.

[Whereupon, at 12:31 p.m., the hearing was concluded.]

○