Testimony of

Mr. Robbie Callaway

September 9, 2003

TESTIMONY OF

MR. ROBBIE CALLAWAY
Chairman

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

On

Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks

For the

U.S. Senate
Judiciary Committee

September 9, 2003

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 regarding the issue of Peer-to-Peer networks as they relate to the distribution of child pornography.

The National Center is intimately involved with the issue of sexual exploitation of children over the Internet, through its Exploited Child Unit and the congressionally mandated CyberTipline - the "911 of the Internet".

The National Center, in partnership with the Federal Bureau of Investigation, Bureau of Immigration and Customs Enforcement, U.S. Secret Service, the U.S. Postal Inspection Service, and state and local law enforcement in Internet Crimes Against Children Task Forces, serves as the Nation's CyberTipline and as the national Child Pornography Tipline. We ask that individuals contact us with information that will help in our fight against child sexual exploitation. The information is forwarded to law enforcement for investigation and review, and, when appropriate, to the Internet service provider. The U.S. Congress has funded these initiatives for reporting child sexual exploitation.

Types of child sexual exploitation that the National Center analyzes include: 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 family); and unsolicited obscene material sent to a child.

As of August 24, 2003, the CyberTipline has received over 145,000 reports regarding various types of child sexual exploitation. The CyberTipline has received 1513 reports regarding child pornography being traded by Peer-to-Peer users.

Several of these CyberTipline reports resulted in the arrest of those individuals who were trading sexually explicit images of children. Interestingly, all of these arrests occurred during 2001 and/or early 2002. We

did not receive any peer-to-peer reports in years 1998-2000, and the peer-to-peer reports grew five-fold between years 2001 and 2002. According to NCMEC records, there do not appear to be any CyberTipline reports during the last year involving Peer-to-Peer networks that resulted in an arrest. One clear reason exists which explains the reduction in arrests:

In recent years, peer-to-peer programs have been making 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 peer-to-peer 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.

It is important to mention that while tracking users trading illegal content on peer-to-peer programs 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, including Naperville, Illinois's Detective Mike Sullivan, have begun to use secondary programs to identify the IP address of the perpetrator sending the illegal files. However, these programs must be active at the exact moment of file transfer. Depending on the 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 an incredible 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 reduce if users knew that recipients of the images/movies could easily attain their IP address.

As I stated earlier, the National Center has received leads on over 1500 peer-to-peer trades of child pornography. I'd like to now demonstrate the National Center's involvement in two cases where there was a successful resolution from peer-to-peer CyberTipline reports:

On April 19, 2001 the CyberTipline received an anonymous complaint regarding child pornography being traded on a peer-to-peer network. During his searches, the caller found a disturbing image that he described as, "two little girls touching themselves below the waist." According to the caller, the girls appeared to be approximately 12 years of age.

NCMEC analysts conducted a search of the peer-to-peer network and found numerous images of child pornography being traded. One individual trading these images was using an IP address registered to the University of California - Santa Barbara. NCMEC contacted UCSB Campus Police.

Subsequently, university detectives, working with the Santa Barbara Sheriff's Department High-Tech Crime Unit, were able to verify the existence and location of the offender. A 21-year old suspect was identified and a search warrant was executed at his apartment located off campus. A forensic search of his computer found numerous child pornography images. The suspect confessed and the District Attorney's Office filed felony charges of distributing child pornography on May 17, 2001.

On May 20, 2002, the National Center received a CyberTipline report referring to a suspect who was trading 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, it was determined that the suspect had connected to the Internet from Manhattan, Kansas.

The National Center contacted law enforcement officials in Kansas and provided them with the documentation of the illegal files being traded from their jurisdiction. 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 involving his own. The suspect admitted to raping, sodomizing and sexually abusing his daughter.

It is unlikely this predator would have been arrested if a concerned citizen hadn't known the correct 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 software programs to allow users to log the origination of files.

A decade ago, FBI Special Agent Ken Lanning, now retired, author of NCMEC's major publications in this field, outlined for Congress why pedophiles collect and distribute child pornography:

1. To justify their obsession for children
2. To stimulate their sexual drive
3. To lower a child's inhibitions
4. To preserve a child's youth
5. To blackmail
6. As a medium of exchange
7. For profit

As Agent Lanning noted, molesters use child pornography to stimulate their own desires and fuel their fantasies for children as sexual partners. Viewing these images whets the appetite of the molester and serves as a precursor to his own sexual acts with children. The more frequently a molester views child pornography, the more he, like his child victims, becomes desensitized to the abnormality of his conduct. He can convince himself that his behavior is normal, and eventually he will need more and increasingly explicit child pornography to satisfy his cravings. When mere visual stimulation no longer satisfies him, he will often progress to sexually molesting live children.

There is compelling evidence that child pornography will cause real physical, emotional and psychological damage not only to those children involved in the pornography, but potentially to children who are shown that child pornography, and who are lured into performing sexual acts because of the reasons that Agent Lanning states, including lowering their inhibitions.

We will all agree that children who are involved in child pornography are, by the very nature of the industry, victims of sexual exploitation and sexual abuse. Ann Wolbert Burgess, of the Boston College Nursing School, states, "The destructive effects of child sexual abuse can create a number of long-term problems for the child victim. Studies of sexually exploited children indicate a variety of long-term emotional, behavioral, social, and sexual problems. Symptoms include physical problems of headaches, stomachaches, and sleeping and eating disorders; psychological reactions of fear and anxiety, depression, mood changes, guilt, and shame; social problems of school truancy, declining grades, and fighting; and sexual problems, such as heightened sexual activity, compulsive masturbation, exhibitionism, and preoccupation with sex and nudity. Running away from home, adolescent prostitution, suicide attempts, substance abuse, gender identity confusion, sexual dysfunction, and socially deviant behaviors have also been identified as possible consequences of untreated childhood sexual abuse."

To summarize, the National Center believes the use of peer-to-peer networks for the distribution of child pornography is a growing problem. We suspect that there is an increase in distribution as pornographers look for lower risk avenues where the possibility of being identified is less. Law enforcement faces 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 moment the offense occurs.
? Individuals from all over the world use these peer-to-peer programs.

The National Center's CyberTipline is the nation's primary vehicle for reporting sexual exploitation of children, and we would be interested in playing an even larger role than we currently do.

I don't have an answer today on how to combat the all-pervasive problem of trading illegal child pornography on the Internet, but I thank you, Mr. Chairman, for calling this hearing to order to begin dialogue on this problem. We look forward to continuing a discussion and analysis of distribution of child pornography on the Internet via peer-to-peer networks.