U.S. House of Representatives
Committee on the Judiciary

Testimony of
Michelle Collins
Director
Exploited Child Division
The National Center for Missing & Exploited Children
for the
United States House of Representatives
Committee on the Judiciary
"Sex Crimes and the Internet"
October 17, 2007

Mr. Chairman and distinguished members of the Committee, as the Director of the Exploited Child Division of the National Center for Missing & Exploited Children (NCMEC), I welcome this opportunity to appear before you to discuss crimes against children on the Internet. NCMEC joins you in your concern for the safety of the most vulnerable members of our society and thanks you for bringing attention to this serious problem facing America's communities.

Let me first provide you with some background information. 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. Our federal funding supports specific operational functions mandated by Congress under Section 5773 of Title 42 of the United States Code, which is attached.

These include a national 24-hour toll-free hotline; a distribution system for missing-child photos; a system of case management and technical assistance to law enforcement and families; training programs for federal, state and local law enforcement; and programs designed to help stop the sexual exploitation of children.

One of our programs is the CyberTipline, the "9-1-1 for the Internet," which serves as the national clearinghouse for investigative leads and tips regarding crimes against children on the Internet. Congress mandated that NCMEC establish and operate the CyberTipline in its Justice Department appropriations legislation for fiscal year 1998, which is attached. The CyberTipline is operated in partnership with the Federal Bureau of Investigation ("FBI"), the Department of Homeland Security's Bureau of Immigration and Customs Enforcement ("ICE"), the U.S. Postal Inspection Service, the U.S. Secret Service, the U.S. Department of Justice's Child Exploitation and Obscenity Section, the national Internet Crimes Against Children Task Force (ICAC) program, and state and local law enforcement.

Leads are received in seven categories of crimes:

- 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);
- unsolicited obscene material sent to a child; and
- misleading domain names.

Since the CyberTipline began operation, NCMEC has received and processed more

than 525,000 leads, resulting in hundreds of arrests and successful prosecutions. These leads come from both the public and electronic service providers (ESP), which are mandated to report under Section 13032 of Title 18 of the United States Code.

Reports are prioritized, processed and submitted to the appropriate law enforcement agency. The FBI, ICE and Postal Inspection Service have "real time" access to the leads, and all three agencies assign agents and analysts to work on-site at NCMEC and review the reports. We are not authorized to send CyberTipline reports to foreign law enforcement agencies. This is a real problem, considering the global nature of the Internet.

Rapid dissemination of CyberTipline reports is accomplished through the use of Virtual Private Network (VPN) connections. ESPs that are registered with the CyberTipline use a VPN to upload images of apparent child pornography directly into our server. These images are encrypted for additional security. The VPN is also used to transmit images and CyberTipline reports to the national ICAC program, which also has a secure, encrypted connection to the NCMEC system.

The majority of CyberTipline leads are referred to the 46 federally funded ICAC taskforce agencies, one of the most effective initiatives in the fight against online child victimization. It was Congress that, in 1997, conceived the idea of creating specialized units to investigate these crimes. In the 10 years since then, the national ICAC program has become a model of successful federal oversight of state and local programs which, though geographically diverse, are united by national standards of investigative policies and procedures. The national ICAC program complements the federal agencies' efforts, as they work seamlessly in the fight against online child victimization.

A typical analysis of an ESP report begins by taking whatever information is in the report and trying to match it to other online activity. Conducting online searches is one method we use to try to connect a real person to the online criminal conduct. We use both publicly-available search tools as well as commercial search tools that are given to us at no cost by our corporate partners.

Because Congress intended the CyberTipline to augment rather than replace established law enforcement procedures, the information we provide is only the first step in the process. Our searches turn up information that is valuable to law enforcement, including whether the perpetrator has legitimate access to children – such as a school bus driver. Law enforcement will want to move quickly in cases where children could be in imminent danger. Using the information we gather, law enforcement serves legal process, gathers evidence, and obtains probable cause to arrest the perpetrator.

An obstacle to this process is that not all ESPs are reporting and those that do report are not sending uniform types of information, rendering some reports useless. Some ESPs take the position that the statute is not a clear mandate and that it exposes them to possible criminal prosecution for distributing child pornography themselves. In addition, because there are no guidelines for the contents of these reports, some ESPs do not send customer information that would allow NCMEC to identify a law enforcement jurisdiction. As a result, potentially valuable investigative leads are left to sit in the CyberTipline database with no action taken.

There is also another necessary yet missing link in the chain from detection of child pornography to conviction of the distributor. Once the CyberTipline analysts give law enforcement all the information they need about specific images traded on the Internet, there can be no prosecution until the date and time of that online activity is connected to an actual person. There is currently no requirement for ESPs to retain connectivity logs for their customers on an ongoing basis. Some have policies on retention but these vary, are not implemented consistently, and are for too short a time to have meaningful prosecutorial value. One example: law enforcement discovered a movie depicting the rape of a toddler that was traded online. In hopes that they could find the child by finding the producer of the movie, they moved quickly to identify the ESP and subpoenaed the name and address of the customer who had used that particular IP address at the specific date and time. The ESP was

not able to provide the connectivity information. To this day, we have no idea who or where that child is – but we suspect she is still living with her abuser.

In the cases we have seen, the child victims would have never told anyone about their abuse, and their perpetrators would have remained anonymous but for the CyberTipline and vigorous law enforcement investigation.

Who are the children in the images we see every day? Of the identified offenders in a one-year period, 83% had images of children younger than 12 years old, 39% had images of children younger than 6 years old, and 19% had images of children younger than 3 years old.

Because of our role as a clearinghouse for online crimes against children, and the reputation we've earned for assistance to law enforcement, our analysts see more child pornography than any law enforcement agency in the world. This benefits our Child Victim Identification Program, a joint project with our federal law enforcement partners and the national ICAC task force program, whose mission is two-fold: (1) to help prosecutors get convictions by proving that a real child is depicted in child pornography images; and (2) to rescue the children. To date we have records relating to almost 1200 identified child victims.

The Internet has become a primary tool to victimize children today, due to its widespread use and the relative anonymity that it offers child predators. The CyberTipline is a tool used by law enforcement to apprehend those who use the Internet to victimize children.

Today, NCMEC is working with leaders in the Internet industry in order to explore improvements, new approaches and better ways to attack the problems. We are also bringing together key business, law enforcement, child advocacy, governmental and other interests and leaders to explore ways to more effectively address these new issues and challenges.

NCMEC urges the Committee to take a serious look at the dangers threatening our children today, and to move decisively to provide law enforcement with the tools they need to identify and prosecute those who target our children.

Now is the time to act.

Thank you.