U.S. House of Representatives
Committee on the Judiciary

Testimony of Executive Assistant Director Michael A. Mason
Of the Federal Bureau of Investigation
Before the
Committee on the Judiciary
United States House of Representatives
October 17, 2007

Good morning Mr. Chairman, Ranking Member Smith and distinguished members of the Committee. I would like to thank you for the opportunity to address the FBI's role in combating the sexual exploitation of children through the use of the Internet.

With more than one billion people around the world routinely online, the Internet has become an integral part of our daily lives. It has dramatically enhanced the way we communicate, the way we learn, and the way we work.

As *New York Times* columnist Thomas L. Friedman wrote in his best-selling book "The World is Flat," the Internet has leveled the playing field, creating a convergence of people, places, knowledge, and information. We have gone global as individuals.

However, globalization has brought about new challenges. Criminals are making ready use of the Internet, engaging in illegal activities ranging from credit card scams, consumer frauds, computer intrusions, money laundering and a host of other illegal activities. Terrorists around the world are recruiting, communicating and planning attacks, aided by laptops and Internet access.

One of the most insidious uses of the Internet is for child sexual exploitation. An increasing amount of this exploitation takes place in the dark shadows of the Internet – on websites and message boards, through file sharing and e-mail, and in real time with web cams and streaming video.

The assault on children is nothing new, however the Internet grants a far greater level of immunity to those who would prey on our children. As a result, there can be no tolerance and no retreat in our efforts to combat this scourge. We cannot and will not rest until these predators are shut down and locked up. That is why coordinated efforts like Project Safe Childhood, which brings federal, state, and local law enforcement and prosecutors together in task forces led by the local United States Attorney to combat online child sexual exploitation, are so important.

Today I want to talk about what we in the FBI are doing to attack child exploitation on the Internet. I want to touch on what we do in terms of evidence collection and prosecution. Lastly, I want to talk about the role of both parents and the private sector in addressing this problem.

One of our most important programs is the Innocent Images National Initiative, which for 11 years has targeted sexual predators who use the Internet to exploit children. Unfortunately, there is no shortage of work in this arena. Between fiscal years 1996 and 2005 there were over 15,556 investigations opened in this program. In 2005 alone, there were over 2,500 cases opened as opposed to 113 in 1996. This represents an increase of 2050%. During this ten year period, investigations under the Innocent Images National Initiative have resulted in 4,784 individuals being charged, 6,145 individuals being arrested, located or summoned to appear in a court of law and 4,822 convictions being obtained.

We have ongoing undercover operations across the country, with more than 240 agents who investigate cases with their state and local counterparts.

On any given day, these investigators may pose as children to lure online predators into the open. They may pose as collectors seeking to share images through peer-to-peer networks. They may coordinate with the National Center for Missing & Exploited Children to identify children and adults featured in child pornography. Or they may train police officers to investigate cases in their own jurisdictions.

With heightened scrutiny in the United States, child pornographers are going further underground, using file-sharing networks and encrypted websites. They are concealing their financial mechanisms through a maze of online payment services, including the use of stolen credit cards. They are traveling to foreign countries to exploit minors. They are victimizing more children, in more ways, at younger and younger ages.

In one instance, agents in Chicago searched a predator's residence and found a customized computer with five hard drives and several external drives. They seized more than a terabyte of digital evidence – the equivalent of more than one million paperback books. This man has been sentenced to 20 years in prison not only for distributing pornography, but for producing images of his own resulting in the victimization of a minor child.

In another such case, a cyber agent traced images downloaded from a file-sharing network to a man in the Pittsburgh area. Together, agents and members of the High Tech Crimes Task Force seized more than 2,500 images of highly graphic child pornography, housed everywhere from the subject's computer to DVDs to his Apple iPod.

These cases are significant not just because of the amount of material seized, but because of our collaboration with state and local counterparts.

This coordination is not limited to the national level. Police officers from Britain, Australia, Belarus, Thailand, and the Philippines, among others, work with agents and analysts on the Innocent Images International Task Force in Calverton, Maryland.

Our international partners know the language, the customs, and the cultures of their home countries. Today, information that once took weeks or even months to relay can be exchanged simply by walking across the room. Together, we have convicted a number of child predators around the world.

For example, last October, Ukrainian investigators arrested a man associated with a young girl featured on a pornographic website. The man had received money and gifts in exchange for allowing the girl to be sexually abused on camera. This investigation started in Denmark, and spread to Ukraine and the United States. It was a Ukrainian police officer, a member of the task force, who played a key part in capturing this criminal and shutting down this website.

Child pornography is a global threat that requires a global response. We have no choice but to work together. It is not just a matter of preference, but of necessity.

As these cases illustrate, identifying child predators is only part of the equation. We must also collect the evidence necessary to convict them.

Our Regional Computer Forensics Labs (RCFLs) and our Computer Analysis Response Teams (CART) work with federal, state, and local officials to find and preserve this vital evidence.

Last year, RCFL examiners working with the San Diego Internet Crimes Against Children Task Force targeted an international ring of child molesters, who distributed photos and videos over the Internet. These individuals victimized at least 45 children, including 37 children from the United States, ranging in age from 2 to 14. Twenty-five individuals in Europe and North America were arrested and tried for their involvement. Examiners spent more than 500 hours collecting the evidence necessary to put these men away.

Unfortunately, such cases are all too common. In the past five years, RCFL and CART examiners have conducted more than 31,000 examinations. As the number of computer crimes we investigate has increased, so has the need for computer forensics.

It is always a struggle to square priorities and improve services with limited resources. We must find a way to balance our forensic needs in counterterrorism, counterintelligence, and computer intrusion cases with an ever-increasing need for such analysis in child exploitation cases.

To meet that need, we have trained more than 16,000 law enforcement officers to handle digital forensic evidence.

FBI digital evidence forensic examiners developed a special tool to aid investigators known as Image Scan. This tool and its training course is one of our most sought-after training programs by both domestic and international law enforcement agencies. This program enables investigators to identify, isolate, and store images from a suspect's computer on a thumb drive without altering the original evidence on the computer.

We have provided Image Scan training to more than 4,600 state and local task force officers, enabling them to collect data necessary to obtain search warrants, or to detain subjects pending a more comprehensive analysis. This year, with the Department of Justice's Computer Crime and Intellectual Property Section, we will train our international partners in Brazil, Budapest, Estonia, Portugal and Canada, to name just a few.

At the same time, the FBI is constantly evaluating, expanding and improving the way that it performs computer forensics and delivers the processed results to investigators. Each year the size of personal computing storage capacity increases while the overall cost drops. The result is that the volume of evidence confronting FBI digital evidence forensic examiners today has become staggering. As of the end of FY 2007, FBI CART reports that it has processed in excess of 2.5 petabytes of data (that is in excess of 2.5 million gigabytes). To combat these trends, the FBI has deployed 25 state-of-the-art forensic networks to major FBI Field Offices. These networks enable FBI forensic examiners to more efficiently process seized digital evidence and then present the results to investigators for their review through their desktop computers.

Despite the unprecedented growth of seized data, the FBI has witnessed a ten per cent reduction for the past two years in the backlog of child exploitation digital evidence examinations as a result of these network efficiencies. Based upon the proposed FY 2008 budget, the FBI plans to expand the forensic networks to an additional ten field offices while continuing to examine smaller network solutions for the FBI's smaller field offices and resident agencies. To enhance our investigative efforts, the FBI's Digital Evidence Section and Cyber Division have recently joined forces to stand up the first digital evidence forensics unit dedicated solely to the processing of Innocent Images evidence. The new unit, expected to be fully operational by the end of FY 2008, will be in Linthicum, Maryland, and will have up to ten full time forensic examiners. It will perform full content forensic examinations on priority investigations.

By giving cyber investigators the tools they need, we are reducing our backlog and leaving more complex matters for the CART teams and the RCFLs.

We know there is a real need for additional training, faster services, and better coordination, and we will continue to expand these efforts in the years to come.

I want to talk for just a moment about the importance of community outreach and private sector partnerships.

Part of our job – and an integral part of Project Safe Childhood – is to educate the public about child exploitation. The Internet has provided child predators with a sense of anonymity and their products a world-wide portability. These are not mere pictures

or posed shots, but live acts of molestation. And as predators become desensitized, those who once collected images may start to create images, seeking to harm younger children, in more terrifying ways.

Our cyber agents routinely meet with members of the community to talk about Internet safety. Parents may not understand the dangers lurking in cyber space, or what they are doing to put themselves and their children at risk. A parent may see a web cam as an easy and inexpensive way for a child to communicate with friends or relatives, but a predator sees it as an open window into a child's bedroom.

In field offices around the country, agents are teaching parents how to protect against the tactics used by predators, and the risks of peer-to-peer file-sharing networks, instant messaging, and social networking sites.

We are also working with the media to get the message out. Our Endangered Child Alert Program, conducted in partnership with the National Center for Missing & Exploited Children and Department of Justice's Child Exploitation and Obscenity Section, uses national and international media exposure to identify unknown predators and victims. Through publicity on the FBI website and the television show "America's Most Wanted," we have identified and arrested eight predators. More importantly, we have identified more than 30 child victims.

In another effort, Oprah Winfrey uses her television show to alert viewers to known sexual predators and posts their faces and identifying information on her website. She is offering $100,000 out of her own pocket for each predator brought into custody. Within the first week, two fugitives were arrested. Since then, two more predators have been taken into custody.

We have also enlisted the help of our private sector partners. We have asked Internet service providers and search engine operators to monitor their websites, and to alert us when they discover illegal content.

We in law enforcement face another hurdle in purging predators from the Internet – and that hurdle is tracking both the criminal and the crime. Data linking criminals to their crimes is absolutely essential in the fight against online child exploitation. We are working with Internet service providers on a voluntary basis to retain records of online activities so that we can identify predators and their activities and successfully prosecute them.

Everyone in this room is familiar with violence and injustice. There are few things more difficult to bear than the victimization of a child. These cases are horrific, heartrending, and seemingly endless in number.

The FBI is committed to protecting the most vulnerable among us. We are committed to sweeping sexual predators off the street, off the Internet, and out of our children's lives.

In closing, I want to recognize those who investigate and prosecute these cases. They deserve our respect, our admiration, and our gratitude. They have seen the darkest side of humanity. However, this is some of the most important work we do.

I would like to thank the Committee for addressing this very important issue and for allowing me to testify. I look forward to answering your questions.