

TESTIMONY

of

ERNIE ALLEN

PRESIDENT AND CEO

THE NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

for the

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

“The Protecting Children From Internet Pornographers Act”

July 12, 2011

Mr. Chairman and distinguished members of the Subcommittee, I welcome the opportunity to appear before you to discuss the Protecting Children from Internet Pornographers Act. We are grateful for the Subcommittee's commitment to the safety of our children.

As you know, the National Center for Missing & Exploited Children ("NCMEC") is a not-for-profit corporation, mandated by Congress and working in partnership with the U.S. Department of Justice. NCMEC is a public-private partnership, funded in part by Congress and in part by the private sector. For 27 years NCMEC has operated under Congressional authority to serve as the national resource center and clearinghouse on missing and exploited children. This statutory authorization (see 42 U.S.C. §5773) includes 19 specific operational functions, among which are:

- operating a national 24-hour toll-free hotline, 1-800-THE-LOST® (1-800-843-5678), to intake reports of missing children and receive leads about ongoing cases;
- operating the CyberTipline, the "9-1-1 for the Internet," that the public and electronic service providers may use to report Internet-related child sexual exploitation;
- providing technical assistance and training to individuals and law enforcement agencies in the prevention, investigation, prosecution, and treatment of cases involving missing and exploited children;
- tracking the incidence of attempted child abductions;
- providing forensic technical assistance to law enforcement;
- facilitating the deployment of the National Emergency Child Locator Center during periods of national disasters;
- working with law enforcement and the private sector to reduce the distribution of child pornography over the Internet;
- operating a child victim identification program to assist law enforcement in identifying victims of child pornography;
- developing and disseminating programs and information about Internet safety and the prevention of child abduction and sexual exploitation; and
- providing technical assistance and training to law enforcement in identifying and locating non-compliant sex offenders.

Our longest-running program to help prevent the sexual exploitation of children is the CyberTipline, the national clearinghouse for leads and tips regarding crimes against children on the Internet. It 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 Military Criminal Investigative Organizations, the Internet Crimes Against Children Task Forces (“ICAC”), the U.S. Department of Justice’s Child Exploitation and Obscenity Section, as well as other state and local law enforcement. We receive reports in eight categories of crimes against children:

- possession, manufacture and distribution of child pornography;
- online enticement of children for sexual acts;
- child prostitution;
- sex tourism involving children;
- extrafamilial child sexual molestation;
- unsolicited obscene material sent to a child;
- misleading domain names; and
- misleading words or digital images on the Internet.

These reports are made by both the public and by Electronic Service Providers (“ESPs”), who are required by law to report apparent child pornography to law enforcement via the CyberTipline (18 U.S.C. §2258A). The leads are reviewed by NCMEC analysts, who examine and evaluate the content, add related information that would be useful to law enforcement, use publicly-available search tools to determine the geographic location of the apparent criminal act, and provide all information to the appropriate law enforcement agency for investigation. These reports are triaged continuously to ensure that children in imminent danger get first priority.

The FBI, ICE and Postal Inspection Service have direct and immediate access to all CyberTipline reports, and assign agents and analysts to work at NCMEC. In the 13 years since the CyberTipline began, NCMEC has received and processed more than 1.1 million reports. To date, ESPs have reported to the CyberTipline more than 8 million images/videos of sexually exploited children. To date, more than 51 million child pornography images and videos have been reviewed by the analysts in our Child Victim Identification Program (“CVIP”), which

assists prosecutors to secure convictions for crimes involving identified child victims and helps law enforcement to locate and rescue child victims who have not yet been identified. Last week alone, CVIP analysts reviewed more than 240,000 images/videos.

The child pornography industry has exploded. New technologies such as smart phones, digital cameras and webcams have made it easier for offenders to produce, access, and trade images. More robust storage devices enable offenders to collect unprecedented volumes of images.

These images are crime scene photos. According to law enforcement data, 19% of identified offenders in a survey had images of children younger than 3 years old; 39% had images of children younger than 6 years old; and 83% had images of children younger than 12 years old. Reports to the CyberTipline include images of sexual assaults of toddlers and even infants.

There are millions of child pornography images being traded online by individuals who view them for sexual gratification. Offenders can access them for free on all platforms of the Internet, including the World Wide Web, peer-to-peer file-sharing programs, and Internet Relay Chat.

There is also another side to this problem: offenders who treat these children as a commodity, profiting by selling online access to child pornography images. Who is behind this? Law enforcement investigations have found that organized crime networks operate some of these enterprises. One such case was that of the Regpay Company, a major Internet processor of subscriptions for third-party commercial child pornography websites. The site was managed in Belarus, the credit card payments were processed by a company in Florida, the money was deposited in a bank in Latvia, and the majority of the almost 300,000 credit card transactions on the sites were from Americans.

This is but one example of the connection between child pornography and the financial system. In response to concerns about child pornography distributors' use of our financial systems, with the urging of Senator Richard Shelby, then-Chairman of the Senate Banking Committee in 2006, NCMEC created the Financial Coalition Against Child Pornography ("Financial Coalition").

The Financial Coalition is an alliance between private industry and law enforcement in the battle against commercial child pornography. It is managed by the International Centre for Missing & Exploited Children (“ICMEC”) and NCMEC. The Financial Coalition is made up of leading banks, credit card companies, electronic payment networks, third party payments companies and Internet services companies. Its members comprise nearly 90% of the U.S. payments industry. Our goal is twofold: (1) to increase the risk of running a child pornography enterprise; and (2) to eliminate the profitability.

In each case NCMEC works hand-in-hand with federal, state, local or international law enforcement, and the first priority is always criminal prosecution. However, our fundamental premise is that it is impossible to arrest and prosecute everybody.

How does the Financial Coalition process work? First, NCMEC identifies apparent child pornography websites with method of payment information attached. Then, the credit card industry works with undercover law enforcement officers to identify the merchant bank involved in the financial transaction. Finally, the merchant bank enforces its Terms of Service to stop the flow of funds to these sites.

The Financial Coalition has given us valuable information about how the commercial child pornography industry has evolved. When the Financial Coalition was launched, it was common to see commercial child pornography website subscription prices of \$29.95 per month, payable by credit card. As law enforcement investigations of commercial child pornography websites increased, the websites evolved, requiring alternative payment methods in a multi-layered verification process involving passwords and text messages. More recently, the Financial Coalition has reported that many of these websites are refusing to accept credit cards from the United States. Now, we have found websites that appear to accept a customer’s credit card information, but actually use the information to steal the customer’s identity, not to sell them child pornography.

The Financial Coalition is critical in the global effort to dismantle enterprises that profit from the heinous victimization of children. What once was believed to be a multi-billion dollar global industry has recently been estimated to be less than a million dollar a year industry worldwide, according to the U.S. Department of Treasury. As the commercial child pornography industry continues to evolve, law enforcement efforts will continue to evolve as well. We urge Congress to ensure that its legislation does not impede the ability of financial companies to work with law enforcement in an effort to fight these criminal enterprises.

NCMEC's CyberTipline receives reports from members of the public and electronic service providers ("ESPs") regarding online crimes against children, making it a major source of leads for many law enforcement agencies. This reporting mechanism helps streamline the process from detection of child sexual exploitation to prosecution and conviction. This process increases the efficiency of law enforcement's efforts and maximizes the limited resources available in the fight against child sexual exploitation. The value of the CyberTipline as a source of leads for law enforcement has been greatly enhanced by the collaboration of ESPs.

The greatest challenge to law enforcement investigating online crimes against children is that technology allows offenders to use the Internet with perceived anonymity. There is a significant missing link in the chain from detection of child pornography to conviction of the offender. For example, once a NCMEC analyst reviews a CyberTipline report, adds necessary information and refers it to law enforcement, there can be no prosecution until law enforcement connects the date and time of that online activity to an actual person – the type of information found in an ESP's connectivity log. Connectivity logs provide the link between an Internet Protocol ("IP") address and an actual person. These records are vital to law enforcement investigating and prosecuting these cases.

ESPs' connectivity logs are analogous to the records that telephone companies are required by federal law to keep -- the date and time that a phone number was dialed.

There is currently no requirement for ESPs to retain connectivity logs for their customers on an ongoing basis. While some have policies on retention, these policies vary, are not implemented

consistently, and may be for too short a time to have meaningful investigative value. As a result, offenders are willing to risk detection by law enforcement, believing that they can operate online anonymously. Federal law requires telephone companies to retain their records for 18 months (47 C.F.R. 42.6).

One example: in a 2006 Congressional hearing an Internet Crimes Against Children Task Force Officer testified about a movie depicting the rape of a toddler that was traded online. In hopes that they could rescue the child by finding the producer of the movie, law enforcement moved quickly to identify the ISP and subpoenaed the name and address of the customer who had used that particular IP address at the specific date and time. The ISP did not retain the connectivity information and, as a result, law enforcement was forced to suspend the investigation. Tragically, the child has never been located by law enforcement – but we suspect she is still living with her abuser.

We recognize that online child exploitation presents challenges for both the Internet industry and law enforcement. However, we are confident that there is a way to balance the needs and priorities of both. Too many offenders have gone undetected by law enforcement and are willing to gamble that they can operate online anonymously. Federal, state, and local law enforcement have become more resourceful, but the lack of connectivity retention presents a significant barrier to their investigations. Please help ensure that law enforcement has the tools they need to identify and prosecute those offenders who are misusing the Internet to victimize children. Too many child pornographers feel that they have found a sanctuary. Let's not prove them right.

Identifying and tracking non-compliant fugitive sex offenders has become one of law enforcement's biggest challenges. The Adam Walsh Child Protection and Safety Act of 2006 tasked the U.S. Marshals Service ("USMS") with apprehending these absconded sex offenders. Since 2006 the USMS has arrested over 1,300 fugitives for violations of the Adam Walsh Act.

One of NCMEC's Congressionally authorized responsibilities is to provide training and assistance to law enforcement agencies in identifying and locating non-compliant sex offenders.

NCMEC analysts run searches of non-compliant sex offenders against public-records databases donated to us by private companies for the assistance of law enforcement. We also conduct internal searches for potential linkages of non-compliant sex offenders to NCMEC cases of child abduction, online exploitation and attempted abductions. We forward all information to law enforcement, who uses it to locate the offenders so they can be charged with the crime of non-compliance.

In 95% of the USMS cases, the fugitive's use of a communication device, such as the Internet or telephone, is the key piece of evidence in locating the fugitive. Currently, U.S. Marshals working to locate fugitives must undertake a burdensome and time-consuming legal process to obtain the Internet information. Timeliness is critical in these cases because the Marshals are trying to locate a fugitive, who by nature is mobile in order to evade law enforcement. The delay in the current process provides a window of time during which the fugitive can move again, evading capture by the Marshals.

The U.S. Marshals are key players in the fight against child sexual exploitation. They have made remarkable progress in tracking down non-compliant sex offenders. However, their efforts would be dramatically enhanced if they were granted administrative subpoena authority.

In conclusion, we would like to thank Chairman Smith and Representative Wasserman Schultz for sponsoring this important piece of legislation. Your efforts will undoubtedly help law enforcement better combat child sexual exploitation.