



# CYBERTIPLINE

## 2005 COMPUTERWORLD HONORS CASE STUDY

### GOVERNMENT & NON-PROFIT ORGANIZATIONS

THE CYBERTIPLINE OFFERS A WORLDWIDE MEANS OF REPORTING INCIDENTS OF CHILD SEXUAL EXPLOITATION AND SERVES AS A TECHNICAL ASSISTANCE RESOURCE CENTER FOR THE PUBLIC, PARENTS, AND LAW ENFORCEMENT REGARDING THESE ISSUES. AS OF DECEMBER 2004, THE CYBERTIPLINE HAS ANALYZED MORE THAN 290,000 REPORTED INCIDENTS. [20055275]

*A Search for New Stories*



Robert Carrigan,  
Chairmen of the Chairmen's Committee

Ron Milton,  
Vice-Chairman of the Chairmen's Committee

Dan Morrow,  
Chief Historian

### SUMMARY

Launched in March 1998, the CyberTipline offers a worldwide means of reporting incidents of child sexual exploitation and serves as a technical assistance resource center for the public, parents, and law enforcement regarding these issues. As of December 2004, the CyberTipline has analyzed more than 290,000 reported incidents.

### APPLICATION

Investigating child-exploitation cases may require specialized technical skills outside the scope of usual investigative methods. In 1996 the U.S. Congress established the Exploited Child Unit (ECU) within NCMEC. The ECU serves as a resource center for the public, parents, law enforcement, and others on the issues of the sexual exploitation of children.

Launched in March of 1998, the CyberTipline offers a worldwide means of reporting incidents of child sexual exploitation including the possession, manufacture, and/or distribution of child pornography; online enticement of children for sexual acts; prostitution of children; child-sex tourism; extra familial child sexual molestation; unsolicited obscene material sent to a child; misleading domain names. The CyberTipline is also federally mandated to receive reports of child pornography from Internet Service Providers (ISP's). The goal of the CyberTipline is twofold: To empower the public to take immediate and direct action to enforce a zero tolerance policy regarding child sexual exploitation and to assist all levels of law enforcement by providing one streamlined reporting tool that enhances information sharing and collaborative efforts to combat these crimes.

Reports can be made to the CyberTipline through the online reporting form located at [www.cybertipline.com](http://www.cybertipline.com) or by contacting the 24-hour Call Center at 1-800-843-5678. The CyberTipline is staffed 24 hours a day, 7 days a week in order to respond to the over 290,000 reported incidents received as of December 2004. Every report made to the CyberTipline is analyzed for content, which may include visiting a website or newsgroup, contacting the reporting person to gather additional information, and/or conducting searches using various Internet tools. When appropriate, the report is then disseminated to federal, state, local and international law enforcement agencies investigating cases of child sexual exploitation for further investigation. Of these reports disseminated to law enforcement, there are thousands of ongoing investigations into possible suspects of child sexual exploitation. In addition, countless CyberTipline reports became the catalyst for the arrest of individuals who committed crimes against children. In many of these cases the further victimization of a child was prevented, as a result of law enforcement investigation of CyberTipline reports. The CyberTipline has become the 9-1-1 of the Internet.

Statistics for CyberTipline reports received the week of 12/13/04 – 12/19/04 and total number of reports to date:

Type of Incident\* Weekly Project to Date\*\*\*

Child Pornography 1,236 267,593

Child Prostitution 6 2,667

Child Sex Tourism 5 1,187

Child Sexual Molestation (not in the family) 15 7,200

Online Enticement of Children for Sexual Acts 43 12,276

Unsolicited Obscene Material Sent to a Child \*\*\*\* 3 1,725

Misleading Domain Name\*\*\*\*\* 20 449

Total # of Reports \*\* 1,328 293,097

\*As selected by reporting person/caller when completing this form.

\*\*Blank Reports (included in total) : 983 (Since March 9, 1998)

\*\*\*Since March 9, 1998

\*\*\*\* Since Sept. 1, 2002

\*\*\*\*\* Since April 20, 2004

In addition to serving the public, the ECU serves as a technical and informational resource for law enforcement. Analysts are available to assist in any child-exploitation case, not just those originating from the CyberTipline. As of December 2004, ECU analysts have responded to over 8,400 requests from law enforcement for assistance. ECU analysts have extensive training in data collection using the Internet, as well as the interpretation of E-mail and newsgroup headers, IP addresses, and WHOIS results. Analysts use Internet resources to gather information about websites, E-mail addresses, newsgroup postings, and suspect locations, in addition to other important pieces of information relating to a case.

The ECU has access to several public-record databases that may yield critical information on suspects such as social security and/or drivers' license numbers, past criminal history, and recent addresses. Further, with the use of a program named Verity, analysts are able to conduct searches on all fields contained within CyberTipline reports in an attempt to determine similarities or trends. All information located by these technological means is provided to law enforcement and has greatly assisted with their cases.

## **BENEFITS**

Reports of child sexual exploitation are at an all time high. Over the past five years, reports to the CyberTipline have increased by 750%. This dramatic increase clearly demonstrates that child sexual exploitation is a major problem in the United States and around the world. The CyberTipline is bridging the gap between the public, the ISP's, and law enforcement agencies helping to crack down on child predators. Further, the increase in CyberTipline reports can also be attributed to an increase in public awareness towards child victimization. The CyberTipline, as the 9-1-1 of the Internet, has provided the public with the necessary information to protect their children and in worst case scenarios provided the means with which to report crimes committed against their children. Through the cooperative efforts of the CyberTipline, law enforcement is being notified about more possible suspects committing crimes of child sexual exploitation than ever before.

In 2003, the CyberTipline received nearly 82,000 reports of child sexual exploitation. This large volume of reports was double the number received in 2002. Since the CyberTipline was created in 1998, the ECU has handled more than 200,000 reports.

### Statistics for CyberTipline's Five-Year History

#### Year Tips Increase

1998 4573

1999 9673 111.5%

2000 19276 99.3%

2001 24460 26.9%

2002 43097 76.2%

2003 81987 90.2%

The rapid growth in child pornography reports can be attributed to the ever-increasing number of users on the Internet, more affordable technology, and a federal law requiring ISP's to report all incidents of child pornography on their systems to the CyberTipline. Each of these reports is provided to law enforcement or one of the federal law enforcement agencies working in partnership with NCMEC: the Federal Bureau of Investigation, U.S. Immigration and Customs Enforcement, U.S. Secret Service, U.S. Postal Inspection Service, U.S. Department of Justice's Child Exploitation and Obscenity Section and the OJJDP-funded Internet Crimes Against Children Taskforces.

The CyberTipline contains a matrix allowing each of these federal partners to have real-time access to the reports. This technology, which is unique to the CyberTipline, allows each agency to share crucial information regarding which reports they will be investigating, thereby decreasing the risk of duplication of efforts. The matrix provides a distinct advantage to law enforcement agencies and has fundamentally changed

how these reports are handled. To minimize duplication of efforts, the CyberTipline/Verity searches also provide an avenue to conduct deconfliction services for law enforcement. Law enforcement resources are already taxed and there is no need to increase this burden by having more than one agency unknowingly working on a target at the same time. The ability of CyberTipline analysts to conduct comprehensive searches benefits law enforcement by allowing them to make quick queries to verify they are not wasting their resources on a target that is already under investigation in another jurisdiction. These two technological advances will only increase the amount of cases of child sexual exploitation being worked by law enforcement around the world.

There is an ever-increasing burden placed on law enforcement to investigate online child sexual exploitation. However, the Internet presents many jurisdictional difficulties. The CyberTipline has expertise in determining which law enforcement agencies have the appropriate jurisdiction to handle the case. Once the reports are provided to the correct law enforcement agency, the CyberTipline analysts continue to follow up until the case has come to fruition providing whatever technical assistance services are necessary. In addition, the CyberTipline also has a database of law enforcement contacts worldwide that can assist in other jurisdictions, states, or countries, if the need arises. There have been countless times in which a suspect in one jurisdiction has victims in many different states or countries. When this occurs, the resources and technical assistance of the CyberTipline analysts and databases prove invaluable so that all possible child victims are protected from further harm.

## **IMPORTANCE**

The CyberTipline utilizes Sun Microsystems Java 2 Enterprise Edition (J2EE) software in a 3-tier architecture: the data tier, the client tier, and the end user tier. The data tier is comprised of Computer Associates' Advantage Ingres database software. Java servlets perform middleware functionality and Java Server Pages (JSPs) make up the client tier. The end user only requires a browser to access the system, whether it is the public reporting a CyberTip, or an analyst reviewing that tip. This configuration is very easy to maintain because changes occur at the server level, rather than at the client level.

The system was developed by a partnership with Sun Microsystems java architects and Computer Associates database experts. NCMEC IT staff now maintain and enhance the software. The system runs on Sun Microsystems hardware with Resonate software performing load balancing between web servers. Web servers accessible by the public reside in a DMZ configuration, partitioned by firewalls from internal web servers and the database. Direct access to the database is allowed only by internal web servers. This adds a layer of security to the system.

Public access to the CyberTipline is through our website, [www.missingkids.com](http://www.missingkids.com) or [www.cybertipline.com](http://www.cybertipline.com). Secure access is provided to our state and federal partners through a Virtual Private Network (VPN) connection.

The CyberTipline allows non-profit, for-profit companies, and state and local law enforcement agencies to collaborate in the fight against the exploitation of children. The CyberTipline facilitates this collaboration by enabling the parties to share information with the use of just a browser and an Internet connection. Prior to the CyberTipline, agencies each had their own system for receiving and processing information, none of which exchanged data with other organizations. The CyberTipline has changed that dynamic.

## **ORIGINALITY**

The CyberTipline is constantly evolving to keep up with the changes in technology and the need for resources in the area of child sexual exploitation. This is one of the most exceptional areas of the CyberTipline. As a need arises, the CyberTipline is there to assist. Research results were released in the publications entitled *Online Victimization: A Report on the Nation's Youth and Internet Sex Crimes Against Minors: The Response of Law Enforcement*, which indicated that children were being aggressively sexually solicited online and were not notifying a parent or anyone else about the incident. Further, research conducted by ADVO Inc. indicated that one in three parents were not concerned about their children's safety online. Armed with this information, the CyberTipline partnered with the Advertising Council to produce a series of public service announcements (PSA) titled HDOP: Help Delete Online Predators. These PSAs were designed to raise public awareness about the prevalence of online sexual exploitation and to help parents and teens better protect themselves from online sexual predators. This PSA campaign was the first national, multimedia campaign to address this issue.

As technology changes so do the ways it can be used to exploit children. Recently, the advent of cameras and electronic messaging has become prevalent among cellular telephones. This type of technology quickly falls into the hands of child sexual predators, which can greatly impact law enforcement investigations. As a result,

the CyberTipline has an emerging technology team that is comprised of three analysts who are conducting research in an effort to determine what pertinent identifying information can be obtained from the header of emails sent from a cell phone and what trainings or programs are available teaching forensic techniques for cell phones. Always staying on top of the most recent technology and trends to better assist law enforcement makes the CyberTipline an amazingly unique resource.

After the passage of 42 U.S.C. § 13032, known as the Electronic Service Providers Act, U.S. Internet Service Providers were mandated to report all incidents of child pornography on their systems to the CyberTipline. This launched the CyberTipline into becoming the only non-profit organization slated to handle reports of this kind. The technology and system was already in place to accept the information and images provided by the ISP's and ensured the quick dissemination of these reports to designated law enforcement agencies. To even further increase the speed with which these reports are provided to the OJJDP federally funded Internet Crimes Against Children Taskforces, U.S. Immigrations and Customs Enforcement field offices, as well Federal Bureau of Investigation field offices, a NCMC Virtual Private Network (VPN) was created. The use of the VPN has streamlined the process of getting crucial time sensitive information regarding crimes of child sexual exploitation into the hands of law enforcement investigators in record time. Although many businesses use VPN technology, its function within the CyberTipline has dramatically increased efficiency as well as rescued children from sexually abusive situations.

## **SUCCESS**

The CyberTipline is a fully functioning program that exceeds its goals every year for assisting the public and law enforcement regarding issues surrounding child sexual exploitation. The number of reports received from the public and ISP's, as well as the number of requests for assistance from law enforcement has increased dramatically each year, which indicates the targeted audience of users has embraced the innovation of the CyberTipline. Based on the statistics from the first five years, it appears these numbers will continue to grow as more people and agencies become aware of the services of the CyberTipline.

Through December 2004 the CyberTipline has received more than 290,000 reports from families, Internet Service Providers, teachers, law enforcement, and many other concerned citizens who want to better safeguard children while they are exploring on the Internet. Many of those leads have taken children out of harm's way.

- A CyberTipline report was received from a member of the public indicating images of possible child pornography were posted in an online group. The CyberTipline analyst accessed the group and verified illegal content posted as attachments to a message. Upon analysis of the header of the message posting, a location of Cincinnati, OH was determined. Through further Internet searches a possible name of the suspect was developed. Utilizing Choicepoint™ public records database searches the suspect's current address, date of birth, and social security number were also developed. The Hamilton County (OH) Sheriff's Office was contacted and provided with the CyberTipline report and all of the analysis. Law enforcement conducted an investigation, contacting the Internet Service Provider and verifying subscriber information. Upon serving a search warrant at the suspect's home it was discovered the suspect had a 7 year-old daughter. The child was removed from the home and thereby rescued from ongoing sexual abuse. The suspect was sentenced to 20 years in prison and the child has since been adopted and is adjusting well in a healthy environment. Law enforcement credits the CyberTipline with saving this child, since they were unaware of the crimes being committed by this suspect prior to receiving the CyberTipline report and analysis.
- A CyberTipline report was received from the concerned parents of a child in Miami, Florida, reporting that a man their daughter had befriended over the Internet was now harassing her over the telephone and via mail. CyberTipline analysts ran searches on the suspect's e-mail address and then using the AutoTrack™ and Accurint™ databases were able to validate the suspect's name and address in Modesto, California. The CyberTipline report was forwarded to the Stanislaus County (CA) Sheriff's Department, and investigators learned the suspect was under investigation by the FBI in Tampa, Florida, for sending sexually provocative materials to a 13-year-old girl. The suspect's computer was seized and investigators found 150 potential child victims he had been communicating with online. So far, the investigation has revealed that this man had victimized eight of these children. The 71-year-old suspect was arrested on 13 felony counts of child molestation, attempted child molestation, and attempted manufacturing of child pornography.
- The CyberTipline was contacted to provide technical assistance after a missing child sent an E-mail to her professor. The 16-year-old girl ran away from her home in Hong Kong and took a flight to the United States. After arriving in the United States her whereabouts were unknown. CyberTipline Analysts reviewed the information in the e-mail's "header" and provided investigators with crucial information about where the child was accessing the Internet. This information directly led to her recovery.

- The CyberTipline received a report regarding newsgroup postings containing pornographic images of children. Analysis conducted on the “header” of the postings provided a possible location for the suspect. The information was forwarded to a local police department, and the suspect was arrested. At the time of his arrest, the suspect had many foster children in his home who were rescued from sexual abuse.
- A CyberTipline report was made regarding a 44-year-old man who had met a 13-year-old child on the Internet. The report indicated the man was headed to an airport to pick the child up. A CyberTipline Analyst conducted extensive searches. The searches revealed the make and model of car the man was driving and the fact he had a criminal history as a convicted child sex offender. Through coordinated efforts among various law-enforcement agencies, the suspect was quickly apprehended before the child was harmed.

## **DIFFICULTY**

As a central clearinghouse tasked with receiving tips from the public regarding child sexual exploitation, we must work with all law enforcement agencies to ensure that the proper jurisdiction receives critical information regarding possible crimes in their area. Recognizing that there are over 18,000 law enforcement agencies in the United States, a great deal of attention is focused on identifying trained law enforcement officers across the country who have the expertise to handle these sensitive cases. In many training programs across the United States, law enforcement officers are learning about the CyberTipline and the vast resources it can provide to their investigations. Each year, CyberTipline supervisory staff provides presentations at some of the most influential conferences on child sexual exploitation in the world.

Each year the total number of reports received has increased dramatically, creating a need for the technology and staff of the CyberTipline to increase at the same rate. Otherwise, the CyberTipline would become paralyzed by its own success. In 2003, the CyberTipline experienced its most significant jump in child exploitation leads receiving nearly 82,000 reports, an increase of nearly 100 percent over the previous year. Continuous changes are being made within the CyberTipline database that allowed for some automation of tasks that would otherwise consume valuable time of the analysts. Further, the total number of staff required to appropriately handle the quantity of reports being received was increased from four in 1998 to twenty-one in 2004. The CyberTipline is constantly evolving and will continue to do so in response to the public and law enforcements need for assistance and resources.

As a result of the passage of 42 U.S.C. § 13032, U.S. Internet Service Providers (ISP's) are mandated to report all incidents of apparent child pornography on their systems to the CyberTipline. It is estimated that there are more than 3,000 ISP's operating within the United States. Large scale efforts were made to educate these companies of this new federal law and what steps they would have to take to be in compliance. Due to the varying architecture of these many companies, the CyberTipline was altered to ensure the receipt of quality information from these companies. One unique feature of the CyberTipline that is only available to ISP's is the ability to receive images of child pornography. For instance, if an ISP determines that particular subscriber posted/transmitted/received child pornography, would be able to provide the CyberTipline with subscriber data as well as the actually illegal images.

At the time the law was enacted, there were no guidelines dictating the type of information provided by the ISP's. The law did not clearly instruct the ISP's as to what information should be included in reports, what format should be used when reporting, or what content could be provided with reports. As a result, each ISP that registered with the CyberTipline was reporting differently. In an effort to streamline the reporting process for the ISP community, CyberTipline management continues to meet with U.S. Department of Justice's Child Exploitation and Obscenity Section as well as with leading members of the ISP community with the hope of creating a “best practices” scenario. This clear line of communication between government officials and private sector companies again demonstrates the effective bridge the CyberTipline is facilitating with the single goal of protecting children from child sexual exploitation.