Child Pornography: Assessing the Global Agenda

14 April 2005

Lyon, France

Child Pornography:
Assessing the Global Agenda

PARTICIPANTS

(organizations and titles are current as of the date of the Lyon Forum)

With special thanks to all the participants for their contributions to the Lyon Forum discussions:

Ernie Allen
President and CEO, International Centre for Missing & Exploited Children

Mary Banotti
Former Member of European Parliament, Ireland
Vice Chair, Board of Directors, International Centre for Missing & Exploited Children

Margarida Barroso
Office of the President, European Commission

Brian Bayliss
Vice President, Risk Management & Security, MasterCard – Europe, Middle East and Africa, United Kingdom

John Brennan
Retired Law Enforcement, Charles River Associates

Daniel D. Broughton, M.D.
Department of Pediatrics, The Mayo Clinic
Vice Chair, Board of Directors, International Centre for Missing & Exploited Children

Florence Bruce
Senior Programme Officer, Child Abuse Programme, Oak Philanthropy, Ltd.

The Honorable Arnold Burns
Former U.S. Deputy Attorney General
Chair, Board of Directors, International Centre for Missing & Exploited Children

Cormac Callanan
Secretary General, International Association of Internet Hotlines (INHOPE)

James A. Cannavino
Chairman, DirectInsite
Member, Board of Directors, International Centre for Missing & Exploited Children

Baron Daniel Cardon de Lichtbuer
Chairman, Board of Directors, Child Focus
Vice Chair, Board of Directors, International Centre for Missing & Exploited Children

John Carr
Internet Advisor, National Children's Home (NCH) Action for Children and Children's Charities Coalition for Internet Safety

Abraham E. Cohen
Chairman and President, Kramex, Inc.
Member, Board of Directors, International Centre for Missing & Exploited Children

Sharon W. Cooper, M.D.
Forensic Pediatrician

The Honorable Dennis DeConcini
U.S. Senator (Retired)
Member, Board of Directors, International Centre for Missing & Exploited Children

Jim Devlin
Vice President, Regional Risk Compliance, Visa International

Tim Del Vecchio
Strategic Police Matters Unit, Organization for Security and Cooperation in Europe

Nancy Dube
Vice President and Chief Operating Officer, International Centre for Missing & Exploited Children

Marie Fletcher
SOS Enfants Disparus

James Gamble,
Deputy Director General, National Crime Squad

Mihaela Geoană
Member, Board of Directors, International Centre for Missing & Exploited Children

Junius J. Gonzales, M.D.
Member, Advisory Board, International Centre for Missing & Exploited Children

Vernon Jones
Red Barnet – Save the Children Denmark

Owen Keenan
Chief Executive, Barnardos

Kristine Kloeck
Director, Child Focus

Irena Kozminska
ABCXXI Emotional Health Program
Secretary, Board of Directors, International Centre for Missing & Exploited Children

Richard C. LaMagna
Director, Worldwide Investigations and Law Enforcement Programs, Legal and Corporate Affairs, Microsoft Corporation

Matthieu Lerondeux
Le Forum des Droits sur l'Internet, French Council of State

Helga Long
Managing Partner, Christian & Timbers
Member, Board of Directors, International Centre for Missing & Exploited Children

Lars Lööf
Head of Children's Unit, Council of the Baltic Sea States

Per-Olof Lööf
CEO, Kemet Corporation
Member, Board of Directors, International Center for Missing & Exploited Children

Carmen Madriñán
Executive Director, End Child Prostitution in Asian Tourism (ECPAT) International

Hamish McCulloch
Director, Trafficking in Human Beings, O.I.P.C – Interpol

Alain Mérieux
Chairman and CEO, bioMérieux
Member, Board of Directors, International Centre for Missing & Exploited Children

Annie Mullins
Global Content Standards Manager, Product and Content Services, Vodafone

Rachel O'Connell
Director of Research, Cyberspace Research Unit, University of Central Lancashire

Carlos Ortiz
Assistant United States Attorney, United States Attorney's Office New Jersey

Valerio Papajorgji
Crimes Against Persons, Serious Crime Department, Europol

Corinne Perben
Secretary General, La Fondation Pour l'Enfance

Juan Miguel Petit
U.N. Special Rapporteur on the Sale of Children, Child Prostitution, and Child Pornography

Maria Reverendo
Special Agent, Criminal Investigations, U.S. Internal Revenue Service

Ruben Rodriguez
Director of Law Enforcement Affairs, International Centre for Missing & Exploited Children

Pamela Shifman
Project Officer, Humanitarian Policy & Advocacy, Office of Emergency Programmes, United Nations Children's Fund (UNICEF)

Mark Sirangelo
Treasurer, Board of Directors, International Centre for Missing & Exploited Children

Christian Sjöberg
Chief Executive Officer, NetClean Technologies

Camille de Stempel
Director of Policy, American Online (AOL) – UK

James M. Sullivan
U.S. National Central Bureau – Interpol

Darshna Tanna
General Manager, Fondation Mérieux

Jean-Christophe Le Toquin
Internet Safety Attorney, Microsoft Corporation - Europe Middle-East Africa

Margareta Traung
Safer Internet Programme, European Commission

Katerzina Zerlinska
Polish Police

Executive Summary

The International Centre for Missing and Exploited Children (ICMEC) hosted its first Child Pornography Forum in Dublin, Ireland in 2002. Experts gathered to discuss issues surrounding child pornography and created a global action agenda known as the "Dublin Plan."[1] ICMEC adopted this plan as its own and has since spearheaded the Global Campaign to Combat Child Pornography. Participants at the Dublin Forum unanimously concluded that child pornography was exploding worldwide and they committed to working together to improve laws, expand knowledge and resources, protect child victims, and target offenders.

On 14 April 2005, ICMEC convened a follow-up forum entitled, "Child Pornography: Assessing the Global Agenda," in Lyon, France (hereinafter "Lyon Forum"). In addition to Members of ICMEC's Board of Directors, the Lyon Forum gathered together experts in the field of child pornography, as well as leaders in the technology and private sectors. The Lyon Forum explored the current state of and emerging trends in child pornography, assessed the progress made on the Dublin Plan, and adjusted its recommendations for future actions accordingly. Discussions at the Lyon Forum conducted addressed law-enforcement initiatives and challenges, government perspectives, victim impact, coordination and collaboration in the non-governmental organization (hereinafter "NGO") spheres, the role of the Internet industry, attacking child pornography as a commercial enterprise, and the role of new technologies in the explosion of child pornography on the Internet.

While Lyon Forum participants (hereinafter "participants") agreed that while considerable, concerted efforts have been expended to combat the spread and dissemination of child pornography, the demand, production, and distribution of child pornography continue to grow at an alarming rate. Participants also recognized that greater measures must be undertaken to protect children from online predators. Participants reemphasized the pressing need for further collaboration and coordination within and across all sectors. The Lyon Forum concluded with participants adapting and updating the 10-point action agenda originally adopted in Dublin three years earlier.[2]

On behalf of ICMEC, I would like to thank our Board of Directors and the participants for their lively dialogue and debate. Thank you for being with us and for your invaluable contributions.

Ernie Allen
President and Chief Executive Officer
International Centre for Missing & Exploited Children

[1] *See* Annex I, *infra*.

[2] *See* Annex II, *infra.*

Lyon Forum Discussions

Statements below are based on dialogue and discussions that occurred over the course of the Lyon Forum.

Law-Enforcement Initiatives and Challenges

Interpol estimates that the number of individuals worldwide who exhibit a sexual interest in children is in the millions, and that figure is growing exponentially. This sexual interest in children, in turn, appears to drive these individuals to continually seek materials and venues in which children are sexually exploited. Investigations carried out in over 100 Interpol Member Countries revealed that offenders operate without fear of apprehension, using their legal names, actual addresses, and credit card information to purchase illegal images of child pornography[3] on commercial web sites.

Thus far, law-enforcement investigative techniques have been centered on offenders, focusing on the seizure of hard drives and the identification of illegal images, and prosecuting those offenders who abuse children and/or who possess and distribute child pornography. Conversely, little effort has been dedicated to identifying the sexually victimized children who appear in these illegal images.

Since December 2004, ICMEC, in conjunction with Interpol and with the support of the Microsoft Corporation, has delivered training around the world to law-enforcement officers on how to investigate computer-facilitated crimes against children. Interpol's role in the trainings includes a victim identification workshop during which Interpol officers outline the methods used to investigate child pornography and to identify victim children. International law-enforcement attendees are provided the opportunity to scrutinize projected demonstrations of actual images and soundtracks and are trained to discern clues specific to their own countries. In fact, in one such training that took place in South Africa, law-enforcement officers recognized the dust on the victim-child's shoes as being the type found in the South African bush. Such clues inevitably help officials track down the possible locations where the abuse took place. In addition to this type of training, Interpol is able to forward images and videos it receives to over 140 Member Countries connected to its I-24/7 communications system in an effort to discern the provenance of these images.[4] To date, Interpol has successfully identified 318 children whose images were collected by Interpol's Child Abuse Images Database. In addition, 14 Member Countries are now – within the restrictions imposed by their national legislations – sharing their data and working proactively to identify victims.

---

[3] The terms "child pornography" and "child sexual abuse images" are used interchangeably throughout this report. Participants at the Lyon Forum expressed concern over the term "child pornography," as it does not accurately convey what the images and moving pictures really are: crime-scene images of a child being sexually exploited, abused, molested, assaulted, raped, etc. However, "child pornography" is the term most widely recognized by the public when referring to such images.

[4] As of June 2006, Member States were connected to the I-24/7 communication system. Through the I-24/7 communication system, Interpol specifically requests Member States to look at such things as architecture of buildings, furniture, marine biology, geology, and products featured in the images, as well as to listen to the language and dialects spoken by the abusers and/or child victims. Additional information on the I-24/7 communication system is available at http://www.interpol.int/Public/ICPO/FactSheets/GI03.pdf.

Despite these ongoing efforts, Interpol recognizes that progress will not be achieved unless it is able to develop a global interactive database that allows law-enforcement agencies in Member Countries to share information about their ongoing child pornography investigations. Interpol estimates that creating and maintaining such a system would cost three million euros. The existing system does not possess share capabilities; therefore, there is an urgent need to invest in an interactive system as the number of participating Member Countries grows.

Furthermore, because the Internet has become the most widely used method of child pornography distribution, many law-enforcement agencies have independently investigated the same leads and images, thus duplicating efforts and unnecessarily expending limited resources. Through the utilization of an interactive system, Member Countries could share information and allow Interpol to coordinate future investigations to prevent redundancy. Duplication would be further minimized at a European level because both Interpol and Europol are already working very closely together. Currently, officers from these two agencies meet on a regular basis to conduct training on investigative techniques and computer forensics. This information sharing ensures they are not investigating the same cases; however, once an integrated, interactive system becomes operational these agencies will be able to instantaneously access the database to see if their cases match any existing ones in the system.

In addition to its investigative powers, Interpol has drafted new resolutions that it intends to submit to the United Nations' General Assembly in 2005. The proposed resolutions are aimed at encouraging countries to enact legislation that target the distribution of child pornography images and that make allowances for the appropriate investigative tools necessary for the successful prosecution of alleged offenders. The fact is that even within certain developed countries certain child pornography offenses are still not criminalized. Some countries refuse Interpol training because they hold the erroneous assumption that participation would be tantamount to admitting the country has child abuse problems. Others deny they have a problem because their law-enforcement agencies have not investigated such child sexual abuse images in the past.

Europol, for its part, strives to better educate the public and law-enforcement agencies in Europe by producing and distributing bi-monthly intelligence reports to European Union (hereinafter "E.U.") Member States. These reports provide updates on the status of child exploitation networks and their modus operandi. Additionally, they highlight the unfortunate absence of child pornography legislation in certain Member States.

In an effort to learn more about the nature of this particular crime, law-enforcement agencies, such as the National Crime Squad in the United Kingdom, the Australian Federal Police, the Royal Canadian Mounted Police, the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement (hereinafter "ICE"), and Interpol, came together as partners to form the Virtual Global Taskforce (hereinafter "VGT")[5]. In the United Kingdom and Australia, for example, the VGT has launched a pilot program to educate the public in recognizing inappropriate online conversations and properly reporting suspicious Internet images. In one instance, a 12-year-old girl was chatting online with a stranger who subsequently invited her for a meeting at a train station. Since this girl had previously watched the launch of the VGT program on television, she was able to visit the web site and follow the reporting instructions contained therein. The details she was able to capture and forward to the VGT ensured the offender's arrest. In this case, the offender had in excess of 40 chat logs involving children on

[5] Additional information on the Virtual Global Taskforce is available at http://virtualglobaltaskforce.com/.

his computer. The analysis of the chat logs revealed that the offender had already met and brutalized a least one of those children. Possessing the national will and sharing law-enforcement resources are proof of the effectiveness of global partnerships to combat child pornography.

Participants also observed that training programs currently offered should be mindful of the differences that exist between legal systems. The investigative methods used in countries with common-law traditions are not appropriate in civil-law systems. For example, in the United States, law-enforcement officers have access to special investigative techniques: they can conduct controlled deliveries, wiretaps, undercover operations, and surveillance with judicial oversight. Such techniques are not available in a number of European and Asian countries.

GOVERNMENT PERSPECTIVE

Participants, whether representing a government agency or not, noted the importance of encouraging and promoting cooperation between government agencies and NGOs in matters concerning both missing and exploited children. Memoranda of understanding in the United States and protocols in Belgium provide the legal framework in which both governments and NGOs have continued to successfully operate.

Similarly, a model protocol for the European Union that takes into account Member States' existing legislation has been drafted and is available for Member State consideration and/or adoption.[6]

VICTIM IMPACT

Child sexual exploitation through child pornography is one of the most difficult forms of child abuse to grasp because most people see it as a victimless crime. Additionally, while there is an immense amount of literature regarding the impact of sexual abuse on children, very little is known about the impact child pornography has on a child whose sexual abuse has been memorialized in photographs, videotapes, or in electronic format for distribution to the general public via the Internet.

The impact of the forced participation of children in sexual abuse images varies with their age. Infants and toddlers do not have much ability to recall their victimization but are at a higher risk for physical trauma when they are sexually abused. There number of images on the Internet depicting infants and toddlers being sexually abused and genitally penetrated is increasing. These infants and toddlers are at a higher risk of contracting infectious diseases, not the least of which is HIV/AIDS, in addition to syphilis and Chlamydia. These diseases overwhelm the immune systems of these children, as they do not benefit from the immunity that older children normally have. Diseases that an older child can recover from are capable of killing an infant or toddler.

Preschoolers (children between the ages of three and five) are increasingly being abused online. These children develop sexualized behaviors that are outside the realm of normal childhood development. Sexualized behaviors in four-year-old children put them at greater risk for re-victimization because they have no cognizance of safety or boundaries. This loss of personal boundaries in children of this age group

[6] Additional information on the proposed European Model Protocol ("Cooperation Between Civil Society Organizations and Law Enforcement Services in the Area of Missing and Sexually Exploited Children: Possibilities and Limits from a European Legal Perspective") is available at http://www.childoscope.net/2006/httpdocs/documents/Model%20Protocol.pdf.

causes them to knowingly or unknowingly convey their own willingness to be with strangers, which puts them at increased risk. In addition, children in the pre-school age group may begin to sexually offend against other children. This is when mutual sexual activity between children starts to happen in part because they are coerced, or groomed, or encouraged to behave in this manner with other children by offenders and also because the normal aspects of sexual exploration that are seen in three-, four-, and five-year-old children become exaggerated when they have been chronically, sexually abused.

As for elementary school-aged children, between five and twelve years of age, the impact is multi-faceted, with the elements of shame and self-blame predominating. These children most commonly demonstrate symptoms of post-traumatic stress disorder, depression, low self-esteem, and eating disorders, and are at increased risk for re-victimization. The victims' perceptions that they may have been viewed in pornographic photography, that others may view them as "bad people," contribute to the sense of isolation that shame and self-blame bring.

Adolescent victims of sexual abuse have a higher incidence of self-injurious behavior: suicide, promiscuous sexualized behaviors, problems with anxiety disorders, and post-traumatic stress disorder. Running away is a particularly insidious behavior because it places adolescent victims at great risk for homelessness and prostitution.

Regardless of age, children whose sexual abuse has been photographed or videotaped and who recognize that they may in fact be seen by others will often acknowledge the sexual abuse but almost categorically deny pictures were taken of the abuse. Furthermore, anecdotal data acquired by the National Center for Missing & Exploited Children (hereinafter "NCMEC") revealed that over 50 percent of the sexually abused children that NCMEC has identified had their pictures taken and posted on the Internet by family members. It is extremely difficult for children in these cases to disclose the abuse and seek the safety to which they are entitled.

Victim children not only carry the horrors and stigma associated with their abuse into adulthood, but some will also grow up fearing they will, in turn, become child abusers. Healthcare professionals today are dispelling the commonly held notion of cyclical abuse. Child sexual abuse victims do not automatically or are even unlikely to become perpetrators, especially if they receive appropriate support. It is incumbent on those whose help child victims to not re-victimize them. Parents, for example, often react poorly when their children report abuse by either denying the abuse or questioning their children's assertions. Asking "are you sure this really happened?" or stating "that is a really bad accusation to come forward with" are not conducive responses on the part of parents, law enforcement, and medical professionals. Furthermore, the idea that children will make false sexual abuse allegations, especially in divorce and custody cases, has been negated.[7]

The online grooming of children and the occurrences of children, especially teenagers, willingly photographing themselves and distributing images via mobile phones and chat rooms are cause for alarm. The online grooming process is typified by three phases: friendship forming, relationship forming, and sexual. The relationship-forming phase often includes the groomer professing love, which is a perfect introduction to the sexual phase. The sexual-phase progresses and often includes descriptions of specific sexual terms and requests for children to engage in those acts and take photographs. Children become

[7] *See generally* Nancy Thoennes and Patricia Tjaden, *The Extent, Nature, and Validity of Sexual Abuse Allegations in Custody and Visitation Disputes*, 14(2) CHILD SEXUAL ABUSE & NEGLECT 151-63 (1990); *see also* Thea Brown et al., *Revealing the Existence of Child Abuse in the Context of Marital Breakdown and Custody and Access Disputes*, 24(6) CHILD ABUSE & NEGLECT 849-85 (2000).

not only the creators but also the distributors of the child sexual abuse images, by posting the pictures on the sites where they met the predators, or by posting them on different sites provided by their abusers.

Ultimately, there is a need to educate children, especially with regard to emerging technologies, such as the picture-messaging mobile phones that are commonly used today. Children are taking and sending suggestive and even pornographic images of themselves to Internet blogs and chat rooms without realizing that they have in fact produced and distributed illegal images. Predators who view these blogs and visit these chat rooms now have easy access to detailed information about the child's routine behavior, thereby increasing the chances the child will be approached and/or abused by the predator.

COORDINATION AND COOPERATION IN THE NGO SPHERE

Over the decades, NGOs have been providing unquestionable leadership in the area of child protection. To deal with the rise of child sexual abuse images on the Internet, the International Association of Internet Hotline (hereinafter "INHOPE") was founded in 1999. To date, INHOPE has brought together 25 hotlines worldwide to:

(1) exchange expertise and reports;

(2) support new hotlines; and

(3) educate the public and policy makers.

Thanks to this type of program, Operation Macy was carried out in Germany, during which a Spanish Internet user reported child sexual abuse images to a participating Spanish INHOPE member. This report led to investigations in 160 countries and resulted in the arrest of 25,000 individuals.[8]

The international global network dedicated to the elimination of commercial sexual exploitation of children, known as End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (hereinafter "ECPAT") International, has counts members in 74 countries. These members are typically grassroots coalitions of NGOs working specifically to combat commercial sexual exploitation of children. In addition to the hotline it operates, ECPAT International strives to improve relations with law enforcement. It also partners with Internet and telecommunications providers to improve the safety of their products.[9]

Save the Children Demark, a staunch advocate of children's rights and a member of the International Save the Children Alliance, has undertaken the important initiative of conducting research into social workers' lack of knowledge and training about Internet-related child sexual abuse images.[10] The United Kingdom counts Barnardos and the National Children's Home (NCH) among its most long-standing and

[8] Additional information on INHOPE is available at http://www.inhope.org

[9] Prior to 1996, ECPAT was known as *End Child Prostitution in Asian Tourism*. Additional information on ECPAT International is available at http://www.ecpat.net/eng/Ecpat_network/history.asp.

[10] Additional information on Save the Children Denmark is available at http://www.redbarnet.dk.

proactive NGOs. These two NGOs currently direct numerous projects in different parts of the United Kingdom dealing exclusively with sexually abused children.[11]

The work carried out by the aforementioned NGOs is not without its challenges. First, there is a concern from a child welfare perspective that conventional child protective services operating in each country through statutory regulations or NGOs tend to disassociate the abuse of children through the Internet from other forms of child abuse and child protection issues. It is unfortunate that even in the cyberspace age, child protective services are still dismissing the Internet as a medium that is beyond their grasp and understanding. A review of casework in the United Kingdom has found that in certain cases the sexual abuse of children was initiated through, or had begun, with the Internet. In these cases, a number of children ended up as subjects of child pornographic depictions while others were groomed and then sexually abused by individuals they first met in an Internet chat room. Efforts, therefore, should be made in the future to involve social workers in training and conferences, which have thus far only included NGOs, law-enforcement officers, government, and Internet providers.

Second, law-enforcement corruption in certain countries hinders the good work carried out by a number of NGOs. The prevailing belief seems to be that there is a better chance of addressing the problem at the national level by bringing it to the attention of international law-enforcement agencies, such as Interpol or Europol, than by dealing with an unconcerned and corrupt local law-enforcement agency.

Third, Internet service providers (hereinafter "ISPs") and Ministries of Communication in a number of countries are flatly unwilling to work or cooperate with NGOs.

Fourth, while traditional Internet connectivity continues to grow, it is being supplanted in African countries, for example, by mobile phones featuring photography options and Internet connectivity. This type of connectivity allows individuals to bypass Internet cafés and home computers and to operate with more mobility and virtual impunity.

Fifth, compared with the international aspect of child sexual abuse images, local Internet abuse cases receive little attention, if any. NGOs need to make a more concerted effort on the local level to expose the public to the child sexual abuse cases occurring in their own communities, all the while empowering children, parents, and teachers with the necessary knowledge and tools to safely navigate the Internet.

Sixth, while it is certainly true that the European Commission has helped finance programs in countries in which none previously existed, its contributions are dwarfed by the contributions of law-enforcement agencies, NGOs, and the technology sector. Furthermore, the European Commission has ongoing relations only with organizations it funds, leaving out a great number of NGOs with which it could share valuable knowledge and expertise.

EXPLORING THE ROLE OF THE INTERNET INDUSTRY

Both the Internet and the mobile phone industries have become proactive and sensitized to child pornography. By building partnerships with law enforcement, designing products that protect children, and educating the public and law-enforcement agencies, they have contributed to the protection of their customers and have set higher standards for their industries. In fact, the Internet has moved from a

[11] Additional information on Barnardos and the National Children's Home is available at http://www.barnardos.org.uk/index.htm and http://www.nch.org.uk/, respectively.

defensive, reactionary approach to leading the global effort in preventing further sexual abuse of children.

In the past, the Microsoft Corporation's partnership with law enforcement focused primarily on protecting intellectual property. Today, however, it boasts a very robust Internet initiative called the Digital Integrity Program. Microsoft provides law-enforcement officers with additional training to enable them to investigate online criminal activities related to child sexual exploitation. Through its partnership with ICMEC and Interpol, Microsoft has sponsored computer-facilitated crimes against children training courses in over twelve countries, benefiting over 700 law enforcement officers.[12]

In addition to law-enforcement training, Microsoft has teamed up with the Toronto Police Service to create the Child Exploitation Tracking System (hereinafter "CETS"). CETS is an all-in-one "dashboard" based on Sharepoint technology designed to enable collaboration, coordination, "deconfliction" (*i.e.*, preventing duplication of efforts), mapping and, search capabilities between law-enforcement agencies investigating child exploitation cases online. This database does not replace existing law-enforcement databases such as those housed at Interpol or Europol. Instead, it enhances their functionality. Furthermore, Microsoft is designing a law-enforcement portal that will provide officers with information regarding child safety and exploitation, legal contacts, and 24-hour forensic support. The forensic support will be available to officers who have seized evidence but who may be experiencing problems with a Microsoft product. Law-enforcement officers will also be able to receive court testimony from Microsoft.

Microsoft continues to shut down sites containing illicit materials and continues to ensure that the products it is developing are not vulnerable to future misuse by sexual offenders. Xbox Live, for example, was designed to allow for parental controls; children may play its games with others online only if parents are present and have consented.

America Online (hereinafter "AOL") has shifted from an adversarial relationship with law enforcement to one of partnership, offering ongoing technical training to law-enforcement agencies in the United States and Europe. AOL also continues to preempt product design flaws in an effort to better protect children online. As for Vodafone, in addition to funding the VGT web site, it has taken proactive steps to prevent its customers from accessing illegal materials. To this effect, and in order to minimize access to illegal materials via their emerging Internet mobile phone services, Vodafone blocks its customers from viewing URLs containing illegal contents, as identified by the Internet Watch Foundation (hereinafter "IWF"). In cases where Vodafone customers attempt to download child pornography images, they will inevitably receive messages from Vodafone warning them that they have attempted to commit a criminal offense and risk criminal prosecution in the future. Those customers who receive unsolicited child pornography images are directed by Vodafone to the IWF Wireless Application Protocol site to report the illegal content.

While these enumerated initiatives are commendable, the Internet industry as well as law enforcement realize that problems continue to emerge. Increasingly, child sexual offenders are perfecting their technical skills, which allow them to continue to exchange child sexual abuse images while hiding their identities. Give that large ISPs keep their logs for a certain length of time, the offenders avoid their use by shifting their attention to smaller ISPs because these providers are not mandated to keep logs for any specific period of time, and consequently they provide offenders with the anonymous haven which they seek. To curb this problem, the United Kingdom, during its 2005 presidency of the European Union, is

[12] These numbers were current as of April 2005. As of October 2006, more than 1,700 officers from 93 countries have been trained.

calling on all 25 Member States to agree on a plan requiring phone and Internet companies to keep client data for at least 12 months.

Another emerging problem concerns "pay-as-you-go" plans, which allow individuals to purchase mobile phones without requiring any type of user registration. This presents a new challenge for investigators; however, many law-enforcement agencies are already working with mobile phone companies to track down terrorists using "pay-as-you-go" methods and hope to achieve the same cooperation with regard to sexual offenders.

ATTACKING CHILD PORNOGRAPHY AS A COMMERCIAL ENTERPRISE

Stopping the commercial sexual exploitation of children is an undertaking that is not for law enforcement and the Internet industry to shoulder alone; it must also involve financial institutions. Online shopping is convenient and affords buyers a sense of anonymity. Sexual offenders not only benefit from this anonymity, but are increasingly adept at finding new ways to avoid detection. A number of credit card companies have responded and instituted a zero-tolerance policy with regard to the use of their credit card logos for the sale and purchase of child pornography on commercial web sites.

Both Visa and MasterCard continue to implement programs and policies to ensure that their products are not used to purchase illegal materials. Contrary to general perceptions, Visa and MasterCard do not directly issue credit cards, nor do they contract with merchants. They do, however, license financial institutions to both issue Visa and MasterCard products and contract with merchants who accept these products. Although Visa and MasterCard do not interface with cardholders and merchants, their role in the process is not marginal because they, and not the financial institutions they license, set the terms surrounding the use of their products. The zero tolerance they have adopted vis-à-vis the use of their products to purchase illegal images exists regardless of whether the countries in which they operate criminalize the possession and distribution of child pornography.

Furthermore, NCMEC and ICE have developed a program that identifies sites supplying child pornography using the logos of credit card companies. This "Cease-and-Desist Program" uses spider technology to identify illegal commercial sites. Once the site is identified, it is reported to NCMEC's CyberTipline and to law enforcement in the United States and the United Kingdom. If law enforcement does not take action, letters are sent to credit card companies notifying them that their services are being misused and to hosting providers warning them of their sites' illegal contents. Visa and MasterCard levy fines on the banks they license as soon as an illegal commercial web site is brought to their attention. This measure is taken in an effort to force these banks to better screen the merchants with whom they transact. These collected fines are in turn invested in programs designated to improve the technology used to identify these illegal commercial web sites.

Commercial child pornography has not only challenged Visa and MasterCard. It continues to challenge law enforcement in their investigations because these sites are easily manipulated; that is, they are frequently created by providing false information to servers and hosting companies. To overcome this challenge, the U.S. Attorney's Office in New Jersey decided to prosecute anyone involved in the commercial operation of illegal web sites and investigators were authorized to make purchases on these commercial web sites. This exercise revealed that while child pornography web sites were quite numerous, very few billing companies were involved in their operations. These same billing companies came up time and again in these investigations. One such company was RegPay, which investigators

determined was generating and moving about one million dollars per month. With the help of Visa, MasterCard, and data processing companies, investigators were able to trace the money to an Internet-based company in Florida called "Connections USA" and "I-Serve." This company was a fly-by-night enterprise operated by four to five individuals. Its primary functions consisted of collecting money that was being processed worldwide and forwarding it to two banks in Latvia, and then to Belarus, for the benefit of RegPay. Following the seizure of I-Serve's database, investigators ultimately discovered that, in addition to providing billing services for hundreds of web sites, RegPay also owned five of the most profitable child pornography web sites that generated 23 percent of its total profits. Consequently, two individuals were extradited from Belarus, pled guilty, and were sentenced to 25 to 30 years in federal prison.

Despite these phenomenal successes and proactive measures, detection will continue to be a challenge in the face of evolving methods of payment. The challenge is to continue this type of detection with the advent of virtual money such as e-Gold. Efforts must intensify and remain ahead of new payment trends.

NEW TECHNOLOGIES AND THE EXPANSION OF CHILD PORNOGRAPHY

Children are unquestionably the clearest targets of these emerging technologies. Children are not incidental purchasing power agents; they have continued to be targeted by the technology industry through the use of extremely savvy, fashionable marketing schemes. Sexual offenders are equally aware of these trends and are quick to acquire the necessary skills that enable them to access, prey on, and, ultimately victimize children. This is why the technology sector must uniformly act in a more responsible manner.

Nonetheless, those entities responsible for protecting children are incapable of predicting new technology trends. INHOPE, for example, is trying to identify the unique challenges that mobile phones, personal digital assistants (more commonly known as PDAs), iPODs, and online gaming pose to hotlines and law enforcement investigating their illegal content. However, at this stage INHOPE can only guess which technology will become the most popular with children. Hence, the technology industry must act proactively and responsibly to form partnerships of expertise with law enforcement and NGOs and develop safer products for children.

Conclusion

At the conclusion of the Lyon Forum, recommendations were made in various categories for ways to better and more effectively combat the scourge of child pornography, especially on the Internet.

Public Awareness

- Raise awareness that child pornography encompasses three types of victimization:
  (1) the act of molestation;
  (2) the memorializing of the act on film or video; and
  (3) the publication of the sexual abuse of children;
- Raise awareness of the effects of each type of victimization on children;
- Raise awareness of the ways the public can report crimes against children;
- Raise political and law-enforcement awareness to secure needed attention and resources; and
- Work to demystify the impersonality of Internet child pornography by increasing public awareness that "the Internet" and "cyber crimes" involve real crimes and real victims.

Offender Awareness

- Encourage prevention by educating potential offenders on the consequences of being involved in child pornography; and
- Promote the levying of aggressive criminal penalties on any offender involved in commercial child pornography operations.

Legal and Law-Enforcement Efforts

- Coordinate law-enforcement investigations to prevent duplication of efforts and waste of resources;
- Promote the adoption of legislation addressing child pornography in countries without adequate laws;
- Build investigative capacity in countries that do not enforce existing legislation; and
- Raise awareness and promote training opportunities for law enforcement internationally.

Victim Identification

- Utilize the more victim-supportive term "child recognition" in conjunction with "child identification" because victims deserve support, treatment, and privacy;

- Promote the exchange of evidence and expertise with Interpol for the purpose of identifying more victims;

- Build investigative capacity in countries not actively identifying victims; and

- Undertake a follow-up study to track-law enforcement responses on the progress of identified child victims.

VICTIM SERVICES AND SUPPORT

- Promote the value of childhood through education and training in areas with little child protection infrastructure;

- Embrace training targeting child protection workers; and

- Promote a unified system of response to child abuse within law-enforcement and child protection agencies.

CORPORATE INVOLVEMENT

- Eradicate the use of credit cards to purchase child pornography;

- Support new mechanisms for reporting illegal accounts to credit card companies and banks as well as for reporting by credit card companies and banks to law enforcement;

- Promote best practices in the area of data retention to allow for proper law-enforcement investigation;

- Encourage smaller ISPs to retain their data by using the support and leadership of the multinational ISPs and ISP associations that are already addressing the issue; and

- Bring the campaign to combat child pornography to the boardrooms of multinational corporations.

Annex I: 2002 Dublin Plan

1. **Build Public Awareness of the Problem of Child Pornography**

   - Create a white paper on the state of the problem.
   - Communicate clearly and aggressively to the public what child pornography really is.
   - Develop a greater public understanding of the cycle of victimization and its implications for public policy and budgets.
   - Create a media-focused campaign.

2. **Demand that Child Pornography Be Placed High on the Political Agenda**

   - Promote the U.N. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Pornography and Child Prostitution.

3. **Create an International Child Pornography Monitoring and Oversight System**

   - Establish an international observatory.

4. **Undertake Extensive Research to Define and Measure the Extent of the Problem**

   - Assess adequacy of definitions and terminology.

5. **Examine and Evaluate Current Law-Enforcement Practices**

   - Identify best practices.

6. **Develop and Promote Systems for Identifying Victims of Child Pornography**

   - Promote greater resources and capacity to support victims.

7. **Develop and Promote Model Legislation to Ensure Consistency of Law among Nations**

   - Provide a clear legislative structure and context for Internet hotlines.

8. **Enhance the Capacity of Law Enforcement to Investigate and Prosecute Child Pornography**

   - Create and promote training, including continuing education.
   - Promote creation of specialized units.
   - Promote creation of multi-jurisdictional task forces.

- Develop Model Protocols to guide law enforcement and prosecutors in child pornography investigations

9. Promote Information Sharing and Coordination between and among Law Enforcement, Internet Hotlines, the Media, and Others

- Promote cooperation, collaboration, and coordination among law enforcement, Internet hotlines, and media outlets.

- Develop an expanded role for media involvement.

10. Promote Stronger Involvement by Private Sector Entities, including ISPs, NGOs, and Others

- Develop partnerships and cooperation with the ISP community.

- Develop an expanded, added value role for NGOs

Annex II: 2005 Lyon Update on the Dublin Plan

1. **Build Public Awareness of the Problem of Child Pornography**

   ICMEC, in partnership with Microsoft and Interpol, is conducting training and roundtable discussions in countries around the world to generate expertise, discussion, and interest.

   Future steps:

   - Raise awareness and educate the public by using more accurate and descriptive terms. Specifically, the term "child pornography" is not "pornography" in the traditional sense; it is pictures of children being sexually assaulted.

   - Promote the value of childhood through education and training in areas with little child protection infrastructure.

2. **Demand that Child Pornography Be Placed High on the Political Agenda**

   ICMEC has attracted political attention to child pornography through roundtable discussions and media interviews.

   Future step:

   - Continue to educate policy makers and the general public about this pervasive and insidious problem.

3. **Create an International Child Pornography Monitoring and Oversight System**

   ICMEC, in conjunction with Interpol, is developing an online resource for child pornography, aptly named the International Resource Centre (IRC). The IRC, found online at www.internationalresourcecentre.org, will be a public resource, with specialized sections for law enforcement.

   Future steps:

   - Perform proactive monitoring of the Internet to identify child pornography trends and potential investigative targets.

   - Expand child victim identification through efforts such as the new International Resource Centre.

4. **Undertake Extensive Research to Define and Measure the Extent of the Problem**

   Substantive and meaningful research efforts have yet to be conducted.

Future steps:

- Conduct a survey of Interpol Member Countries that measures the extent of the problem worldwide.

- Undertake a follow-up study to track law-enforcement responses on the progress of identified child victims.

6. Examine and Evaluate Current Law-Enforcement Practices

It is unclear whether any one person or organization has undertaken the task of evaluating law-enforcement practices.

Future steps:

- Identify and create an international network of experts.

- Develop and promote best practices for investigators.

- Host focus groups on best practices for identifying child victims through technology.

6. Develop and Promote Systems for Identifying Victims of Child Pornography

Interpol and NCMEC are currently operating programs that focus specifically on victim identification.

Future step:

- Increase the worldwide effort to identify children victimized in child pornography and ensure that they receive help and support.

7. Develop and Promote Model Legislation to Ensure Consistency of Law among Nations

ECPAT has done extraordinary work in providing legal definitions and an appropriate framework for legislation. ICMEC has begun the process of evaluating legislation in all Interpol Member Countries.

Future step:

- Ensure that every nation enacts legislation to criminalize the distribution and possession of child pornography and to mandate the reporting of child pornography by ISPs.

8. Enhance the Capacity of Law Enforcement to Investigate and Prosecute Child Pornography

ICMEC, in conjunction with Interpol and Microsoft, is working to train law-enforcement officers from around the world on how to investigate computer-facilitated crimes against children.

Future steps:

- Expand law-enforcement presence online and eliminate the opportunity for sexual offenders and predators to operate in virtual anonymity.

- Enhance law-enforcement expertise and investigative capacity around the world.

9. Promote Information Sharing and Coordination between and among Law Enforcement, Internet Hotlines, the Media, and Others

ICMEC is coordinating focus groups in Europe in collaboration with INHOPE to raise awareness, promote information-sharing and coordination, and urge the adoption of action plans in locations not adequately addressing issues of child pornography. Focus group participants include representatives from law enforcement, Internet hotlines, and the media.

Future step:

- Focus on mechanisms for coordinating law-enforcement efforts to prevent duplicating efforts and wasting resources.

10. Promote Stronger Involvement by Private Sector Entities, including ISPs, NGOs, and Others

In addition to law enforcement, Internet hotlines, and the media, the European focus groups mentioned above will also bring together private sector entities, including, but not limited to, ISPs, NGOs, and other representatives from civil society and the government.

Future Steps:

Corporations

- Work to eliminate the use of credit cards to purchase child pornography on the Internet in order to erode and ultimately eradicate its commercial viability.

- Raise awareness of the ethical consequences for multi-national financial companies.

- Develop processes for the detection and reporting of apparent child pornography in the financial industries.

- Urge financial institutions and credit card services to adopt zero-tolerance policies with regard to child pornography.

- Engage and involve leading banks, credit card companies, major banking associations and organizations, including the World Bank and the International Monetary Fund.

- Develop procedures for asset forfeiture that benefit organizations providing services and support to victims worldwide.

Internet and Technology Providers

- Anticipate the convergence and integration of new technology.
- Work with industry to make safer new products.
- Promote more uniform new technology standards.

NGOs

- Engage grassroots organizations to team up with law enforcement and private industry.
- Work to strengthen NGO efforts and partnerships in countries with little or no police accountability.
- Build partnerships with NGOs to promote children's issues locally and internationally.

Charles B. Wang International Children's Building
699 Prince Street
Alexandria, Virginia 22314-3175 USA
Tel. + 1 703 274 3900 Fax +1 703 549 4504
www.icmec.org