Global Alliance Against Child Sexual Abuse Online

2015 REPORT

Global Alliance Against
Child Sexual Abuse Online

2015 REPORT

Foreword by
Attorney General Loretta E. Lynch

2015 Report: Global Alliance Against
Child Sexual Abuse Online

Child sexual abuse online is a heinous practice that has no place in a civilized society. Whether it involves production, distribution, trade, possession or viewing of child pornography via the Internet, or the online grooming and enticement of minors, these crimes harm our children, devastate our communities, and degrade our world. As our nations become more interconnected than ever before – and as new technology makes it easier to store and transfer electronic data – reducing the circulation of child pornography images across jurisdictional borders grows ever more challenging. Abusers are increasingly operating in international online groups that employ sophisticated technologies and security protocols to conceal perpetrators' identities, allow them to exploit children with impunity, and complicate the efforts of law enforcement. Savvy international offenders also take advantage of law enforcement vulnerabilities caused by differences in laws and policies across jurisdictions – producing not just a jurisdictional gap, but a chasm of justice.

Put simply, this is a global problem that requires a global response. That's why my predecessor, Attorney General Eric H. Holder, Jr., joined with former European Union Commissioner for Home Affairs Cecilia Malmström three years ago to launch the Global Alliance Against Child Sexual Abuse Online. This important effort united high-level decision-makers from all around the world to reaffirm our determination to investigate instances of abuse, to prosecute online offenses, and to put an end to online child exploitation once and for all. On December 5, 2012, forty-eight nations issued a Ministerial Declaration articulating the founding principles of the Global Alliance – and since that time, the Alliance has grown to include fifty-four member states. In September 2014, the United States hosted the Second Global Alliance Ministerial Conference, bringing together high-level government officials,

subject-matter experts, and representatives from law enforcement, non-governmental organizations (NGOs), and the private sector to share notable accomplishments and discuss the most important challenges we continue to face. At the conclusion of the conference, all fifty-four member states endorsed a Ministerial Declaration in which we pledged to address, through a series of concrete actions, the trans-border obstacles to protecting victims of exploitation and prosecuting those who have attempted to exploit them. And through our role as Secretariat of the Alliance, the United States is working to identify the key issues faced by Global Alliance members, and to promote the most effective strategies to overcome those challenges.

The 2015 Report of the Global Alliance Against Child Sexual Abuse Online is a vital part of that effort. It enables all Global Alliance members, as well as other states that look to the Alliance for leadership, to obtain a holistic view of global efforts to eradicate the online sexual abuse of children. It provides detailed information to help bolster technological resources and to communicate best practices. And it transforms one of the greatest impediments to fighting child sexual abuse online – the increasingly international nature of the crimes – into an investigative asset.

Of course, while it is clear from this report that we have made tremendous progress, it is also evident that a great deal of hard work remains to be done. Our challenges are complex, and our goals will not be achieved overnight. That is why the members of this Alliance – and every member of the international community – must continue to work collaboratively, to engage effectively, and to move forward together as we seek to end child exploitation online and build a safer, more secure future for every child around the world.

Loretta E. Lynch
United States Attorney General

Introduction and Report Methodology

Global Alliance members established ambitious goals for the first two years of the Alliance, and identified four broad "policy targets" with corresponding "operational goals" and "action plans":

- **Policy Target 1:** Enhancing efforts to identify victims whose sexual abuse is depicted in child pornography, and ensuring that they receive the necessary assistance, support and protection;

- **Policy Target 2:** Enhancing efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders;

- **Policy Target 3:** Increasing public awareness of the risks posed by children's activities online, including the self-production of images; and

- **Policy Target 4:** Reducing the availability of child pornography online and the re-victimization of children.

Following the launch of the Alliance, member states submitted reports documenting preexisting actions, and actions they committed to undertake in the immediate future, to advance these four key policy targets. In December of 2013, the European Commission published a report summarizing those commitments. Available online at:

http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/global_alliance_report_201312_en.pdf

This Report represented a "collective promise for action." *Id.* at p. 1.

Global Alliance members have, during the past two years, fulfilled that collective promise, often by embracing technology-based solutions to the challenges posed by criminal offenses that are committed in whole or in part on the Internet. Reports published in 2014 and 2015 document the tremendous progress made by each Alliance member. Available online at:

http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/index_en.htm

These reports reflect each state's individual approach to addressing each of the four collective policy targets.

Regarding the first policy target, member states reported on the continuous expansion of Interpol's International Child Sexual Exploitation (ICSE) database of known child abuse images, including the creation of a "worst-of" list of images illegal in every participating country, which will enable more effective monitoring and investigation of contraband files shared over peer-2-peer networks and facilitate the identification of more victims, regardless of national origin. Member states also focused on supporting victims during and after criminal prosecutions via the creation and expansion of programs dedicated to working with online sexual exploitation victims.

> Many members reported increases in the volume of arrests and convictions of online child exploitation offenders, including sophisticated offenders who have taken extraordinary measures to shield their identities and offenses from law enforcement.

Several Alliance members have contributed to the second policy target by adopting new laws broadening the scope of prosecutable conduct within their borders, including criminalizing online enticement or grooming for the purpose of facilitating subsequent sexual abuse. And many members reported increases in the volume of arrests and convictions of online child exploitation offenders, including sophisticated offenders who have taken extraordinary measures to shield their identities and offenses from law enforcement. Member states highlighted the increased

role of international cooperation in many investigations of online offenders operating in multiple jurisdictions.

To address the third policy target, member states employed a variety of creative approaches to increase public awareness of the risks faced by children online. Many states created multimedia, interactive educational materials to reach vulnerable minors through the same online and social media platforms where they are most likely to be approached by offenders. Member states also trained educators, police officers, and others on the front line of the battle against online child exploitation regarding how best to convey to children the threats posed by Internet use.

Finally, Alliance members achieved great progress in addressing the fourth policy target by reducing the availability of child pornography online and reducing re-victimization of depicted minors. Member states facilitated reporting of online child sexual abuse by private citizens, and collaborated closely with the private sector to expeditiously identify and remove child pornography hosted on the Internet.

This Report provides a detailed summary of the progress Alliance members have made in relation to each of the four broad policy targets. Although many member states had implemented measures that addressed some or all of the four policy targets prior to the formation of the Alliance, this Report focuses in large part on each member state's progress since the inception of the Global Alliance, rather than on preexisting accomplishments.

Like the European Commission's 2013 Report summarizing member states' prospective commitments, this Report is organized by policy target and corresponding operational goal. Accomplishments reported by various members are referenced in the discussion of each goal, with the caveat that an accomplishment may be listed only once in this Report even if it may implicate two or more policy targets. This Report summarizes individual member state accomplishments and is not intended to be a comprehensive recitation of each member state's accomplishments. Instead, this Report highlights some of the most significant and innovative accomplishments of the past few years, and also focuses on widespread measures adopted by many Global Alliance members. The Global Alliance website includes full details on the progress of all member states.

Global Alliance Members

ALBANIA

ARMENIA

AUSTRALIA

AUSTRIA

BELGIUM

BOSNIA & HERZEGOVINA

BULGARIA

CAMBODIA

CANADA

COSTA RICA

CROATIA

CYPRUS

CZECH REPUBLIC

DENMARK

ESTONIA

FINLAND

FRANCE

GEORGIA

GERMANY

GHANA

GREECE

HUNGARY

IRELAND

ISRAEL

ITALY

JAPAN

KOSOVO

LATVIA

LITHUANIA

LUXEMBOURG

MALTA

MEXICO

MOLDOVA

MONTENEGRO

NETHERLANDS

NEW ZEALAND

NIGERIA

NORWAY

PHILIPPINES

POLAND

PORTUGAL

REPUBLIC OF KOREA

ROMANIA

SERBIA

SLOVAKIA

SLOVENIA

SPAIN

SWEDEN

SWITZERLAND

THAILAND

TURKEY

UKRAINE

UNITED KINGDOM

UNITED STATES

POLICY TARGET 1

Enhancing efforts to identify victims and ensuring that they receive the necessary assistance, support and protection

OPERATIONAL GOAL

Increase the number of identified victims in the International Child Sexual Exploitation images database (ICSE database) managed by INTERPOL by at least 10% yearly

Action #1 |

Mainstreaming victim identification into investigations and prosecutions.

Identifying victims depicted in child pornography images is a goal central to any online child exploitation investigation. Victim identification is often critical to successfully apprehending and prosecuting offenders, and it is always a prerequisite to removing victims from ongoing abusive situations and to subsequent provision of therapeutic and rehabilitative services.

Member states consistently reported an increased emphasis on victim identification throughout the course of investigations and prosecutions. For example, the United Kingdom's National Crime Agency enhanced its dedicated victim identification resources, resulting in the near-doubling in a one-year span (April 2013 through April 2014) of the number of images depicting unidentified victims submitted by United Kingdom law enforcement to its national database, which is discussed further below. Japan identified a record-high 646 child pornography victims in 2013, many of whom were victims of particularly serious offenses; 70% of newly-identified child pornography victims of elementary school age were also victims of indecent assault or

rape. In the United States, the Department of Homeland Security-Immigration and Customs Enforcement-Homeland Security Investigations (DHS-ICE-HSI)'s National Victim Identification System application contributed to the identification of more than 2000 child pornography victims in 2013 and 2014. Sweden's National Bureau of Investigation Against Child Sexual Abuse Online played a coordinating role for Sweden's 21 regional police services and deployed additional investigators specifically dedicated to the identification of victims. The Netherlands implemented a policy shift regarding its child sexual abuse investigative units to focus more on identification and rescue of victims.

Several member states, including Belgium, Denmark, Slovenia, and Sweden, reported on the ongoing development of and participation in the Netherlands-led IN-4-MATION project, which will connect each participating state's domestic national child exploitation image database to enhance each participant's victim identification efforts. Other member states, including Albania and Austria, also highlighted ongoing close collaboration between domestic and foreign law enforcement in the field of victim identification.

Action #2 |

Improving use and content of the ICSE database.

Managed by INTERPOL, the International Child Sexual Exploitation (ICSE) database allows specialized investigators to share intelligence and leads with colleagues around the world. As of April 2015, the database includes information on more than 6300 identified child pornography victims from over 40 countries, as well as many unidentified victims. The database includes both victim images and the hash values (a string of characters that an image or video file uniquely generates; essentially, digital DNA) associated with each victim. ICSE uses image comparison software to make connections between victims, abusers and the location of offense conduct. Certified users in member countries are able to access the database directly and in real time, thereby providing immediate responses to queries related to child sexual exploitation investigations.

Since 2012, many member states began contributing to the ICSE database, while others have substantially increased the number of images submitted to ICSE and their reliance on ICSE to support and further investigations. The total number of identified victims contained in the database more than doubled between the end of 2012 and April 2015 (from 2891 to 6301). States including Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Hungary, Ireland, Israel, the Republic of Korea, Lithuania, Montenegro, Portugal, the Slovak Republic, and Spain all reported new or

expanded access and contributions to the ICSE database. Furthermore, the majority of member states, including Estonia, Germany, Italy, Luxembourg, Mexico, New Zealand, the Netherlands, Norway, Spain, the United Kingdom and the United States continued to regularly submit images to the ICSE database. For example, the volume of identified United States victims increased from 962 at the end of 2012 to 2778 by April 2015. The United Kingdom's National Crime Agency encouraged increased utilization of the database by disseminating ICSE hash sets to every United Kingdom police force. Those agencies were then able to cross-reference efficiently all domestically-maintained hash sets against the ICSE database to enhance victim identification efforts. Many member states signaled an intent to contribute to an ongoing ICSE initiative in which INTERPOL will create a baseline list of images that satisfy every participating state's definition of child pornography (the "worst-of" list).

Several states, including Austria, Hungary, New Zealand, Poland, Switzerland, the United Kingdom and the United States, offered training dedicated to victim identification techniques, including utilization of the ICSE database. For example, the Criminal Intelligence Service of Austria provided training on victim identification to its national police force, and the United Kingdom Embassy to the Kingdom of Cambodia and the National Crime Agency's CEOP (Child Exploitation and Online Protection) Command jointly provided training related to victim identification to Cambodian police officers.

POLICY TARGET 1

Action #3 |

Improving forensic capabilities.

A number of states, including Albania, Belgium, Cyprus, Hungary, Norway and the United Kingdom, dedicated additional resources to expanding forensic capabilities focused on victim identification. New Zealand, in addition to creating a state-specific victim identification database, developed an online database of school uniforms to aid in the identification of victims. Norway distributed a specialised software/hardware solution, designed to reduce the time needed to evaluate image and movie files, to all local police forces. Belgium employed a new forensic tool that enables investigators to focus on images containing unidentified victims when examining an enormous collection of child exploitation images seized from an offender. In the United States, the National Center for Missing and Exploited Children (NCMEC) operates a Child Victim Identification Lab where eligible law enforcement users observe background identifiers and audio clues from child pornography cases, and are able to leave notes if they detect anything in the images that might help locate the victim. The Netherlands is currently pursuing various technological enhancements related to child identification, including facial recognition, computerized age determination, and software that enables investigators to identify the origin of exploitation images. Albania is investing in improved software for automatic image analysis to speed up the forensic process and to eliminate the need to manually examine each child pornography image.

The United Kingdom's National Crime Agency trained specialist officers in all local police forces regarding the use of NetClean Digital Investigator, which it provides free to law enforcement. This image analysis tool focuses on the child pornography images most likely to hold clues related to their initial production, thereby enhancing victim-identification efforts. Other member states, including Cyprus, have also widely used the NetClean investigative tool. In 2014, the United Kingdom also developed a single, secure national database of child exploitation images, accessible to all local police forces, which categorizes images to increase the efficiency of investigations and enable law enforcement to devote more resources to victim identification.

The United States implemented Project Vic to enhance the investigation of child pornography images that depict unidentified victims and to promote more effective and efficient data exchange efforts in child pornography investigations. The project employs forensic and image categorization tools and other new technologies to facilitate more efficient analysis of computer media containing large collections of child pornography. In 2014, Project Vic trained over 300 students through in-person, hands-on courses and reached hundreds more through domestic and international webinars. United States federal and state law enforcement agencies, non-governmental organizations (NGOs), academics, and private sector entities including Microsoft and NetClean all participate in this initiative. In September of 2014, Project Vic convened its first International Tech Summit, which featured a wide variety of participants from Australia, Canada, New Zealand, the United Kingdom and the United States.

In 2014, Project Vic trained over 300 students through in-person, hands-on courses and reached hundreds more through domestic and international webinars.

Action #4 |

Improving victim assistance, support and protection.

Many member states have augmented an array of rehabilitative services available to assist and protect child victims, and have worked to ensure that police investigations and courtroom proceedings are conducted in a manner that limits the negative impact on victims. A number of states created or expanded special holistic victim centers that gather various services (medical, legal, psychological, educational and social work) together in one child-friendly environment. These centers help to limit the number of times that a victim has to report the details of a crime, and thus limit the trauma associated with reporting. These victim centers also ensure that appropriate therapeutic and medical assistance is available throughout all stages of the investigative and adjudicative process.

For example, Denmark established five special Children's Houses, which draw together social services, police, therapeutic services and health services for abused children. The Republic of Korea established a variety of different specialized centers, including: (1) the Sunflower Children's Center, a national network of eight institutions that provide a "one-stop" center for medical, legal, and psychological services to child victims; (2) Smile Centers, institutions that provide psychological support to child victims and their families as well as serving as temporary shelters for victims; and (3) the Crime Victim Support Center, which provides financial support to the victims of sexual assault and their families. Turkey restructured its "Care and Social Rehabilitation Centers" as "Child Support Centers" to provide specialized service for child victims of sexual abuse. Hungary created child-friendly interview rooms at police stations, to minimize the negative impact of questioning on children, and expanded the array of psychological support services provided to victims. Israel's Assistance to Sex Violence Minor Crime Victims' Law ensures that a child victim of a sexual crime is entitled to immediate assistance in one of five crisis centers operating throughout the country. In 2013, more than 1000 children were treated in these crisis centers. Canada's Child Advocacy Centres coordinate the investigation, prosecution and treat-

ment of child exploitation while helping abused children. These facilities have proven to reduce the trauma that child victims may encounter in the justice system while lowering the length of time required to make charging decisions. Luxembourg and Poland both cooperate on an ongoing basis with non-governmental organizations providing support to child victims and their families.

Members also augmented their policies and procedures focused on protecting victim privacy. Israeli law prohibits the publication or exposure of anything that might identify a minor victim or witness, including the victim's voice, image, name, address, or other identifying traits, and allows courts to conduct otherwise-public hearings involving minors behind closed doors. In early 2014, the Canadian government introduced a Victims' Bill of Rights Act, which secures, among other rights, a victim's right to security, privacy, restitution, and participation in the criminal justice process.

Japan integrates comprehensive psychological services to victims or potential victims in the education and criminal justice environment as both preventative and treatment measures. In many prefectural police departments, Japan employs juvenile guidance counselors to work directly with child victims and to train police officers who work with these victims. Japan also directly intervenes with, and provides specialized psychological counseling to, juveniles posting inappropriate online messages, such as an offer of commercial sex. Japan installed child and family support centers, which provide support for child victims, in 98 locations across the country.

POLICY TARGET 2

Enhancing efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders

OPERATIONAL GOAL

Establish the necessary framework for the criminalization of child sexual abuse online and the effective prosecution of offenders, with the objective of enhancing efforts to investigate and prosecute offenders

Action #1 |

Comprehensive substantive criminal law.

Member states recognize that effective legislation is required to successfully investigate and prosecute those who abuse and exploit child victims online. Many states, including Albania, Armenia, Belgium, Denmark, Estonia, Finland, Hungary, Ireland, Japan, the Republic of Korea, Malta, Montenegro, Nigeria, Romania, Spain, Slovenia, Turkey, Ukraine and the United Kingdom, recently adopted or amended laws to address perceived loopholes in existing domestic legislation. Many of these laws newly criminalized specific categories of online child exploitation. For example, Belgium, the Czech Republic, Montenegro, and Malta newly established grooming of minors for unlawful sexual purposes as a criminal offense. In 2013, Estonia enacted legislation that criminalizes the watching (without downloading) of child abuse material. Denmark amended its Criminal Code to prohibit convicted sexual offenders from contacting children online. Japan criminalized the act of possessing or storing child pornography for the purpose of satisfying one's own sexual curiosity and the act of producing child pornography via surreptitious recording. In Nigeria, the Child Rights Act, signed into law in 2013, criminalized a wide variety of online and of-

fline child abuse and exploitation. In 2014, Switzerland amended its laws to prohibit the viewing of child pornography depicting victims under 18 years of age; previously, only victims under 16 were protected. The United Kingdom proposed legislation that would criminalize the possession and creation of written materials that contain advice regarding how to commit sexual offenses against minors.

Several member states focused on strengthening penalties for online child exploitation offenses. The United Kingdom boosted the sentencing guidelines for offenses involving indecent images of children. In 2015, Canada's Tougher Penalties for Child Predators Act and New Zealand's Objectionable Publications and Indecency Legislation Bill both increased the potential sentences for certain sexual offenses victimizing minors to ensure those penalties reflect the seriousness of the crime.

POLICY TARGET 2

Action #2 |

Removing procedural hurdles.

Several member states committed to improving the efficiency and effectiveness of investigations and prosecutions of child sexual abuse online. For example, Germany's newly-enacted Act on Intensifying the Use of Videoconferencing Technology in Court Proceedings and Investigations by the Public Prosecutor's Office expands the possibilities of interviewing witnesses using video technology. The Polish Parliament is considering proposed amendments to the penal law that would allow for the use of covert surveillance to support the investigation of all sexual offenses against minors.

Action #3 |

Disqualification, treatment, and prevention of repeat offending.

Member states implemented a variety of measures to prevent and deter recidivism and to keep children safe from potentially dangerous offenders following release from incarceration. Latvia amended its Protection of the Rights of the Child law to include an obligation to perform a background check on people who will perform voluntary work that involves direct interaction with minors. The amended statute also prohibits those convicted of sex offenses or other violent crimes from performing voluntary work in child care, education, or health care occupations. New Zealand introduced a mandatory criminal history screening procedure for adults who work with children. Finland amended its legislation to extend criminal screening procedures already in place for adults performing paid work involving children to those who work with children on an unpaid basis. The Republic of Korea expanded the scope of sex offenses triggering an obligation to register in a public database, and developed a Smartphone application that enables more effective browsing of sex offenders' personal information. Israel prohibited minors who perpetrated sex offenses from employment in certain jobs, such as camp counselors. The United Kingdom launched an International Child Protection Certificate (ICPC) program, which helps protect children from British nationals intending to travel overseas for purposes of sexual exploitation by advising prospective overseas employers of an applicant's relevant convictions.

POLICY TARGET 2

OPERATIONAL GOAL

Improve the joint efforts of law enforcement authorities across Global Alliance countries to investigate and prosecute child sexual abuse online

Action #1 |

Improving capacity and coordination of law enforcement authorities.

Member states recognize the importance of training law enforcement to improve capacity to combat child sexual abuse online. Many states, including Albania, Armenia, Austria, Cambodia, Croatia, Estonia, Germany, Hungary, Israel, Japan, the Republic of Korea, Mexico, Montenegro, the Netherlands, Poland, Slovenia, Spain, Switzerland, the United Kingdom and the United States, expanded training for investigators, prosecutors and the judiciary. These trainings focused on both expanding domestic capabilities (e.g., in Albania, Republic of Korea, and Switzerland) and learning from other states' best practices (e.g., in Austria, Cambodia, and Croatia). For example, Armenia published a "Juvenile Justice in the RA" Manual, which is designed to train officers of the RA Police Educational Complex working with minors. Israel established a Joint Experts' Committee that includes prosecutors and police investigators in charge of cyber-crimes. The United States Department of Justice trains 61 coordinated Internet Crimes Against Children (ICAC)
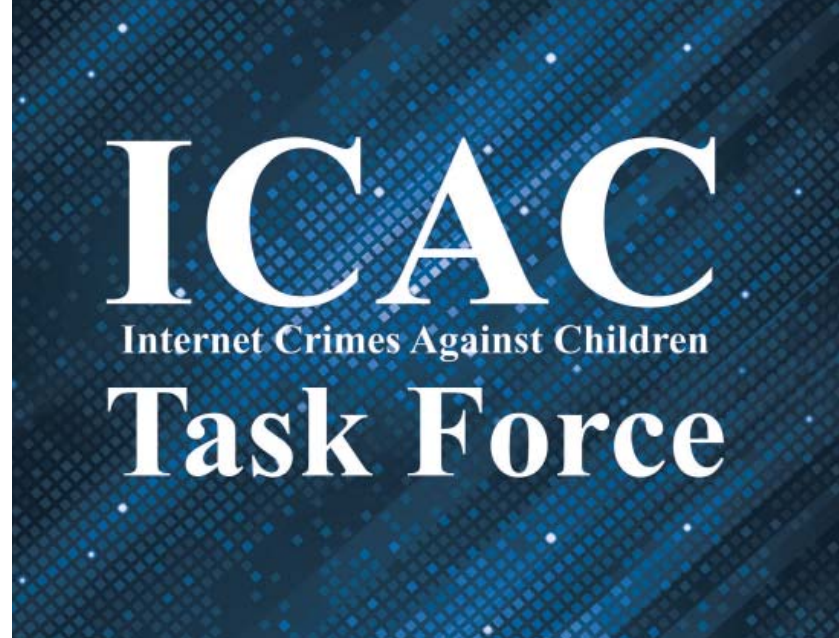
task forces representing more than 3,000 federal, state and local law enforcement and prosecutorial agencies.

Albania, Germany, Hungary, and Japan improved the tools available for police investigations of online child sexual abuse. For example, Germany implemented a pilot program that distributes a national collection of hash values of known child pornography to local law enforcement, while Hungary increased the forensic technical equipment available to its National Bureau of Investigation High-Tech Crime Unit. Albania provided its law enforcement authorities with software, such as EnCase and FTK Imager, to improve the speed in which images are analyzed. The Netherlands implemented a joint knowledge and information sharing center for police and prosecutors, which aims to develop new tools and policies for the investigation and prosecution of sexual abuse. Several members, including the United States and France, reported improved capabilities and investigative techniques for apprehending child pornography offenders operating on the "Darknet," which is composed of networks of Internet technologies and platforms that provide anonymity for users (e.g., TOR).

Action #2 |

Increasing international operational and strategic cooperation.

Nearly every member state highlighted increased cooperation with foreign law enforcement agencies in order to improve investigation of cases of online child sexual abuse. This cooperation is in some cases informal in nature, and in others is facilitated by formal multinational working groups or agencies, such as the Virtual Global Taskforce, EUROPOL, INTERPOL, the FBI's Violent Crimes Against Children International Taskforce, and the IN-4-MATION project.

The Virtual Global Taskforce, for example, is comprised of international law enforcement agencies and private sector partners from around the world, including Australia, Canada, Italy, the Republic of Korea, the Netherlands, New Zealand, Switzerland, the United Kingdom and the United States. This taskforce strives to make the Internet safer by identifying and locating children at risk, and holding perpetrators accountable through timely international collaboration. Several Virtual Global Taskforce member law enforcement agencies (including agencies based in Australia, Canada, Italy, New Zealand, the United Kingdom, and the Netherlands) established their own virtual private network (VPN) connection with NCMEC's CyberTipline to allow direct referrals

of CyberTipline reports to the pertinent investigative agency. Through these connections and other means, NCMEC referred hundreds of thousands of leads to international law enforcement agencies in the past year.

In 2013, the United Kingdom and the United States jointly organized the G8 Global Symposium on Preventing the International Sexual Exploitation of Children to promote cooperation among G8 members' various law enforcement agencies. A number of member states reported new or extended involvement in other international task forces: for example, New Zealand and Cyprus both reported involvement with the FBI's Violent Crimes Against Children International Task-force; Italy and Canada (as a third party contributor) reported participation in Europol's TWINS working group, which facilitates collaboration among member states in combating traveling sex offenders and the production and distribution of child pornography; Slovenia joined Europol's Project HAVEN (Halting Europeans Abusing Victims in Every Nation), which aims to detect and disrupt traveling sex offenders originating from the EU who exploit children both inside and outside Europe; and Switzerland joined EUCTF (the European Union Cybercrime Task Force).

Action #3 |

Improving cooperation with other public authorities and the private sector.

Many member states reported close collaboration with NGOs, Internet service providers (ISPs), and other non-profit or private sector entities regarding the elimination of online child sexual exploitation materials and the apprehension of those responsible for producing and disseminating that material. Albania's National Agency for Computer Security (NACS) and the Authority of Electronic and Postal Communications (AEPC) signed a Memorandum of Understanding for cooperation in this regard, as did the NACS and the Commissioner for Personal Data Protection (CPDP). Luxembourg reported that, while its national legislation has yet to formally regulate the cooperation between law enforcement authorities and private actors, private actors have fully cooperated with the government regarding the elimination of online child sexual exploitation material pursuant to the current system's "honor code."

Please also refer to Policy Target 4 for a more extensive discussion of initiatives to improve coordination across sectors.

POLICY TARGET 3

Enhancing efforts to increase public awareness of the risks posed by children's activities online, including grooming and self-production of images that result in the production of new child pornography that may be distributed online

OPERATIONAL GOALS

Develop, improve, or support appropriate public awareness campaigns or other measures which educate parents, children, and others responsible for children regarding the risks that children's online conduct poses and the steps they can take to minimize those risks

Share best practices among Global Alliance countries for effective strategies to inform the public about the risks posed by online, self-exploitative conduct in order to reduce the production of new child pornography

Action #1 |

Creating awareness-raising materials, channels and campaigns.

Almost all member states have reported progress in developing awareness-raising materials (Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Canada Cambodia, Croatia, Cyprus, Denmark, Estonia, Finland, Germany, Greece, Hungary, Ireland, Israel,

POLICY TARGET 3

Japan, the Republic of Korea, Kosovo, Latvia, Lithuania, Luxembourg, Malta, Mexico, Montenegro, the Netherlands, New Zealand, Nigeria, Norway, Poland, Portugal, Romania, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom and the United States).

The theme for the 11th international "Safer Internet Day," celebrated in February of 2014, was "Let's create a better Internet together." The event encouraged all stakeholders – children, parents, care-takers, teachers, educators, industry and politicians – to work together to cooperatively build an Internet that is safe for children. Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, the Republic of Korea, Latvia, Lithuania, Malta, Montenegro, Netherlands, New Zealand, Nigeria, Norway, Poland, Portugal, Romania, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, and the United Kingdom all participated in this event. For a detailed report on 2014's Safer Internet Day activities:

http://www.saferinternetday.org/c/document_library/get_file?uuid=434bb7df-f0f2-4370-b6d7-ae28d1a6d0e6&groupId=10136 for a detailed report on 2014's Safer Internet Day activities.

A majority of member states implemented targeted information campaigns and made resources more widely available to parents, children, and teachers. For example, Armenia, Austria, Canada, Cyprus, Denmark, Hungary, Ireland, Japan, Montenegro, New Zealand, Portugal, Romania, Turkey and Ukraine published awareness-raising materials for children, teachers and parents. Belgium, Cyprus, Estonia, Portugal, Romania, and the Slovak Republic developed interactive educational tools, such as quizzes, videos, animated series, and advertisements, designed to engage children directly. The Dutch police host a weekly online Q&A, during which children can ask questions about online sexual abuse. Romania organized workshops for parents and their children on the steps they can take to reduce the risks that children face online, and developed a viral YouTube video campaign featuring a video spot, "what did you use to do when you were 7 years old." The video used nostalgia to focus adults on the novel dangers confronting their children in today's Internet-dominated landscape.

In the United States, DHS-ICE-HSI launched a new smart phone application designed to seek the public's help in apprehending fugitive and unknown suspected child predators via anonymous tip reporting. DHS-ICE-HSI also launched an educational outreach program called Project iGuardian, which instructs minors and parents how to stay safe from online sexual predators. In addition, since 2012, more than 175,000 students have completed the FBI's "Safe Online Surfing Program," which addresses dangers associated with online activity.

POLICY TARGET 3

Many member states developed educational initiatives specifically for child audiences. For example, Israel instituted a national "Schools' Week for the Elimination of Sexual Violence," which focuses on the exposure of minors to sexual content on the Internet, and highlights the risks involved with self-production of explicit photographs. Finland's National Institute for Health and Welfare launched a campaign entitled "My body. It's my decision," which raised minors' awareness of how to protect themselves against sex crimes through law enforcement-led educational programs in schools. Malta's "BeSmartOnline!" initiative provided training for all students between 10 and 14 years of age in public, private, and church-based schools regarding digital footprints and digital citizenship, while also promoting Malta's child exploitation help line. Belgium's "Child Focus" initiative informed children about the safe use of the Internet through educational tools, including prevention spots focused on sexting, an online self-test illuminating enticement risk factors, an online application focused on distinguishing online grooming from safe online chats, and an online game that exposes the dangers of sharing private information on the Internet. The United Kingdom distributed and published in English, Thai, Vietnamese, and Khmer more than 20,000 copies of a comic book called "Tam's Tales" that serves as a tool to teach children about protecting themselves from sexual abuse.

Many EU nations participated in the ongoing Safer Internet project (from which Safer Internet Day derived), which promotes Internet safety for children via the development of online and telephonic helplines, and educates and equips teachers, parents and child protection specialists to protect children from evolving technological threats.

A number of other states engaged in similar initiatives, including:

- Austria's "Click & Check" project

- Estonia's "Smartly on the Web" project

- Germany's "Klicksafe," "LOOK- at what your child is doing with the media," and "Surfing Without Risk" initiatives

- Latvia's "Net Safe Latvia Project"

- Lithuania's "You never know who is on the other side" campaign initiated by its Children Support Center

- Luxembourg's "Don't Look Away" project

- Poland's "Internet and the safety of children and young people," "Digital layette for adults," "Digital literacy training," and "Digital Society" projects, each of which focused on different aspects of promoting online safety for children

- United Kingdom's "Thinkuknow" program, which educated more than 3.6 million children in 2014 on the risks that young people face in an online environment

In line with these efforts, many member states, including Belgium, Croatia, Cyprus, Denmark, Estonia, Hungary, Ireland, Latvia, Luxembourg, Malta, the Netherlands, Norway, Portugal, Romania, the United Kingdom and the United States, reported newly developing, augmenting or devoting additional resources to national hotlines dedicated to the reporting of suspected online child sexual abuse.

Action #2 |

Research on trends and threats.

A number of member states, including Albania, Denmark, Estonia, Ireland, Japan, Lithuania, Montenegro, Nigeria, Poland, Portugal, Sweden, and the United Kingdom, dedicated resources to gathering data and reporting on recent trends affecting child sexual abuse online. Estonia, for example, researched its citizens' awareness, attitudes, and behavior with respect to Internet safety. In March 2014, Save the Children Denmark issued the "Images in the Grey Area" report based on data obtained from a domestic hotline for reporting child sex offenses. That report highlights the abuse of children as objects of adult sexual fantasies in "model" or "posing" images, and also addresses online grooming of minors. The United Kingdom is a co-driver of the European Union's Self-Produced Images and Risk Taking Online (SPIRTO) project, which aims to develop a better understanding of self-generated indecent images of children online.

Ireland's Internet Service Providers Association commissioned research on parental attitudes towards children's online safety. This research highlighted widespread parental non-involvement in issues related to Internet safety, at times resulting from a lack of parental knowledge about technology, in general, and social media, in particular. The study also found that only some parents provide guidance to their children concerning Internet use. Ireland widely publicized these results in 2014 with hopes of enhancing parental involvement in children's online lives.

Austria, Belgium, Croatia, the Czech Republic, Luxembourg, the Netherlands, and Switzerland all conducted research on emerging threats to minors, in particular sexting and online grooming. In addition, some states focused research on preventative measures. For example, in 2013, a Japanese study group published "Safety and Security Enhancement Strategies for Smartphones," which recommended best practices for child protection on mobile devices based on studying minors' patterns of usage.

A number of member states, including Albania, Denmark, Estonia, Ireland, Japan, Lithuania, Montenegro, Nigeria, Poland, Portugal, Sweden, and the United Kingdom, dedicated resources to gathering data and reporting on recent trends affecting child sexual abuse online.

Action #3 |

Training.

A number of member states integrated into professional development and other educational programs specific training on risks posed by children's online behavior. These trainings occur at both the national and the international level, and facilitate the dissemination of information to professionals who regularly engage with minors and an exchange of best practices between countries. Israel's Ministry of Education, for example, operates the Unit for Sexuality and Prevention of Harm for Children and Youth, which provides intensive trainings for school counsellors, teachers and educational teams on the prevention of sexual abuse on the Internet as well as general Internet safety. During the 2014-15 school year, Israel trained over 500 school psychological counselors regarding sexual abuse, including online abuse, in addition to more than 500 who had previously received such training; this training is, in turn, imparted to teachers and students throughout the Israeli school system.

Other states engage in similar initiatives. In 2014, Romania published a School Guide on Safer Internet, which provides teachers and caregivers with easy-to-understand theoretical prevention resources, reinforced by practical applications that do not require the use of computers. Albania's Ministry of Education and Sports trained 600 teachers in online safety for children. Belgium's Child Focus provided "Clicksafe" training courses for professionals working with young people. The Police College of Finland offered a two-week course focused on "Sexual crimes and the child in policing." In Hungary, the Biztonsagosinternet Hotline provides on-demand training for children, teachers and parents that address current Internet security topics. The Republic of Korea held "On-Site School Parent Education," and the Turkish National Police Cyber Crime unit offered seminars and conferences at schools around the country. Turkey trained 400 teachers to become specialists in safe Internet usage, and they in turn trained an additional 52,000 teachers. Thailand's Ministry of Education partnered with Microsoft to launch a "Partners in Learning" online community that promotes knowledge sharing among teachers and safe Internet use by students. This initiative also developed and disseminated a comic book to teach the general public, in particular children, about the dangers of Internet use.

Cambodia conducted and attended workshops and meetings, both domestically and internationally, to exchange and share experiences and lessons learned and to develop strategies for combating child sexual abuse online. Cyprus, Japan, Poland, and Romania also reported participation in international conferences, working groups, technical committees and training programs. The United Kingdom established the International Child Protection Network (ICPN), which provides an extensive program of child safeguarding training across the globe for professionals working with children.

POLICY TARGET 4

Reducing as much as possible the availability of child pornography online and reducing as much as possible the re-victimization of children whose sexual abuse is depicted

OPERATIONAL GOAL

Encourage participation by the private sector in identifying and removing known child pornography material located in the relevant State, including increasing as much as possible the volume of system data examined for child pornography images

Action #1 |

Improving cooperation with the private sector.

Cooperation between the public and private sectors is essential to identify and expeditiously remove child exploitation materials from the Internet. Accordingly, many member states have passed legislation or utilized less formal mechanisms designed to encourage ISPs to eliminate child pornography from their systems and to collaborate with law enforcement to identify those responsible for disseminating contraband. Cyprus, for example, imposed a legal obligation on ISPs to restrict access to websites containing child pornography, even without a court order, if they are duly informed by a competent authority or otherwise gain knowledge of child exploitation materials on their systems. Greece implemented similar legislation. Bulgaria invited representatives from its five largest Internet providers to participate in a conference addressing the obstacles to countering online child sexual abuse. All of the representatives agreed to participate in a pilot program that aims to develop a model for blocking certain domain addresses. Cambodia re-

ported that government officials held regular meetings with ISPs to address online child exploita-tion issues. Japan supported the implementation of the "Guideline Regarding Measures against Illegal Information on the Internet" and the "Model Terms and Conditions for ISPs Concerning Illegal/Harmful Information Generated by Users." Montenegro and Spain each established pub-lic-private partnerships requiring ISPs to sign an agreement to block child pornography located on their systems. Sweden directed additional resources to its Financial Coalition against Child Pornography, which works to stop Internet-based payments for child sexual abuse material, and also joined the umbrella European Financial Coalition.

Many states facilitate private industry's efforts to locate and eradicate child pornography via in-formation sharing. For example, beginning in 2013, Switzerland provided its law enforcement's database of hash values of identified child pornography images to Microsoft and Facebook to enable the companies to conduct voluntary searches for those images. This dovetails with those companies' United States-imposed legal obligations to report any child exploitation material dis-covered on their systems to NCMEC. The United Kingdom shared with Google and Microsoft a list of terms used by offenders searching for child sexual exploitation images, enabling those companies to (1) introduce changes to their search engines to prevent images, videos, or path-ways to such material being returned based on those searches and (2) provide clear messages, which appear whenever a blacklisted term is entered into a search engine, warning users of legal consequences and directing them to charities focused on addressing paedophilic predilections. Canada shared PhotoDNA signatures collected from all child pornography images seized by Ca-nadian police with a major social network to facilitate blocking, removal and reporting of those images.

Norway was the initial creator of INTERPOL's worst-of list, which is a compilation of Internet domains that contain clearly and universally illegal child sexual abuse material. INTERPOL provides this list, which is updated several times a week, without cost to any ISP willing to participate in this voluntary initiative. The providers stop all access to these sites, redirecting viewers to a "stop page" or an error message. Similarly, Canada's Project Cleanfeed shares a regularly-updated list of specific foreign-hosted Internet sites associated with child pornography with participating ISPs. In 2014, Japan provided lists of websites containing child pornography to 48 ISPs, three search engines, and three filtering services.

The Republic of Korea employs a three-pronged approach that relies upon government, ISPs, and end-users in equal measure. The Korean Communications Standards Commission, which doubled its monitoring staff in 2013, monitors the Internet for illegal material and recommends that ISPs block identified child exploitation images. Major ISPs, together with the government, established the "Voluntary Censorship Cooperation System" to encourage operators to proactively block child pornography prior to its review by the Standards Commission. In addition, the government has provided, free of charge, filtering software for PCs and screening services for smartphones to millions of end users (approximately 1.5 million smartphone users in 2012 and 2013 alone) to protect minors from harmful materials, including pornography. Thailand completed a similar initiative, developing two software tools – one to facilitate reporting of suspicious websites, one that protects minors from accessing pornographic content – which it disseminated to schools nationwide.

Action #2 |

Development and use of technologies and training to identify and remove child pornography images.

The overwhelming majority of member states have invested in software that is capable of identifying known child exploitation images. As these investments continue to grow, a number of states are taking additional steps to develop novel technological solutions to facilitate the identification of child exploitation materials on the Internet. In 2013, the United Kingdom and the United States established the joint UK-US Taskforce to Counter Online Child Exploitation to harness the expertise of the technology industry to develop technical solutions to counter online child sexual exploitation. The second taskforce meeting, in May 2014, included the largest ever gathering of the technology industry for this purpose: 48 companies and 67 technical experts met over two days, culminating in the collaborative identification of eight innovative technology-based solutions to reducing the availability of child pornography online. In addition, the Netherlands collaborated with social media sites, such as Twitter, to identify and remove newly-discovered child pornography from the Internet as quickly as possible via new technology, including PhotoDNA.

> The overwhelming majority of member states have invested in software that is capable of identifying known child exploitation images.

OPERATIONAL GOAL

Increase the speed of notice and takedown procedures as much as possible without jeopardizing criminal investigations

Action #1 |

Improving cooperation with the private sector on notice and takedown.

Notice and takedown procedures refer to a process in which a content host, after having been informed of child pornography on its system ("notice"), removes such content ("takedown"). Many member states have enacted legislation requiring, or entered into agreements requiring, ISPs to immediately report and remove any child pornography images that they learn are hosted on their servers. For example, pursuant to France's Central Office of Combating Cybercrime agreements with ISPs, in 2013, ISPs removed child pornography from their systems in response to over 25,000 reports of illegal content. To support this initiative, in 2014 France developed, in cooperation with various public and private-sector stakeholders, an online guide directing ISPs how best to respond to discovery of child pornography on their servers. Lithuania's Ministry of Interior promoted a cooperation agreement between the Communications Regulatory Authority and the Police Department which provides for a notice and takedown procedure. The Netherlands reported that its voluntary notice and takedown procedure is 95 percent effective, but a number of "bad hosters" regularly fail to comply with takedown requests. To address this problem, the Netherlands is developing a program called "Cleaning Up Holland," through which law enforcement and relevant partners will work together to improve compliance.
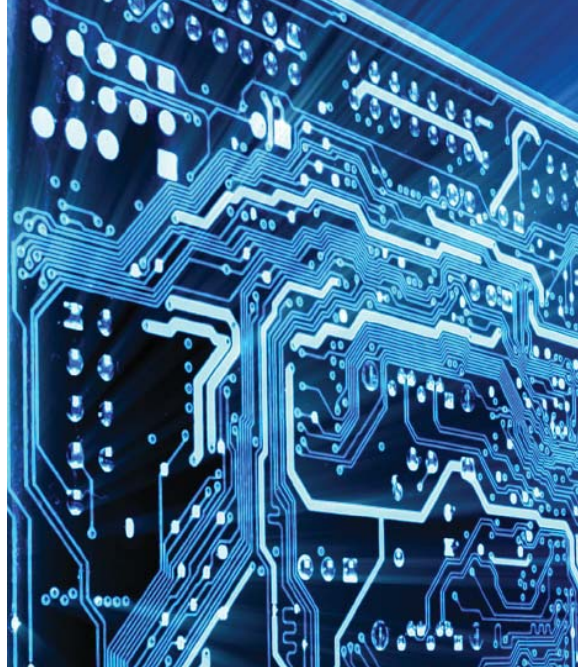
POLICY TARGET 4

Germany collaborated with the INHOPE (International Association of Internet Hotlines) network to optimize the efficiency of notice and takedown procedures. INHOPE is a network of 51 hotlines in 45 countries worldwide that is committed to stamping out child pornography from the Internet. In 2013, 80% of more than 4000 websites hosted in Germany containing child pornography were deleted within two days of identification, and 99% within one week. After two weeks, no child pornography could be retrieved from any of the sites. Luxembourg's collaboration with INHOPE also resulted in improved notice and takedown procedures.

In the United States, NCMEC is actively engaged in notice and takedown measures through its Notice Tracking Initiative, which sends notices of URLs containing apparent child pornography to the relevant domestic or international ISP. ISPs utilize that information to enforce their terms of service, and in 2014, providers removed content, on average, 26 hours after receiving notification from NCMEC.
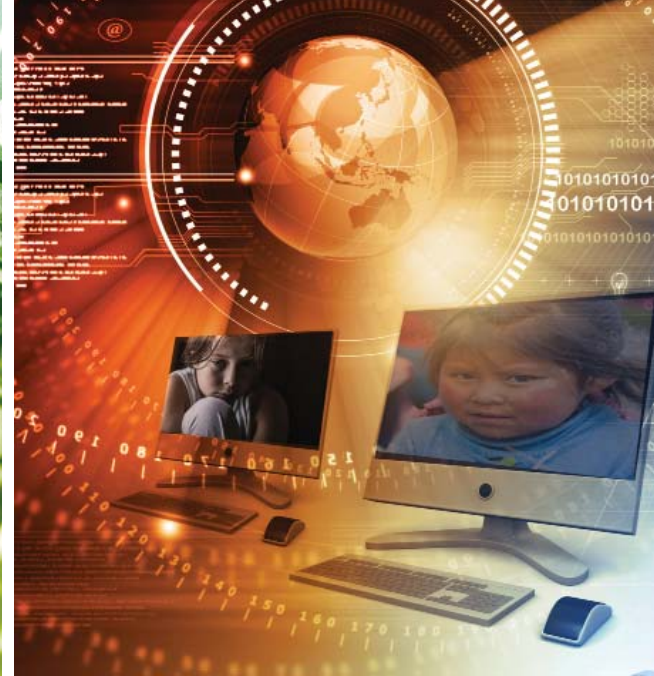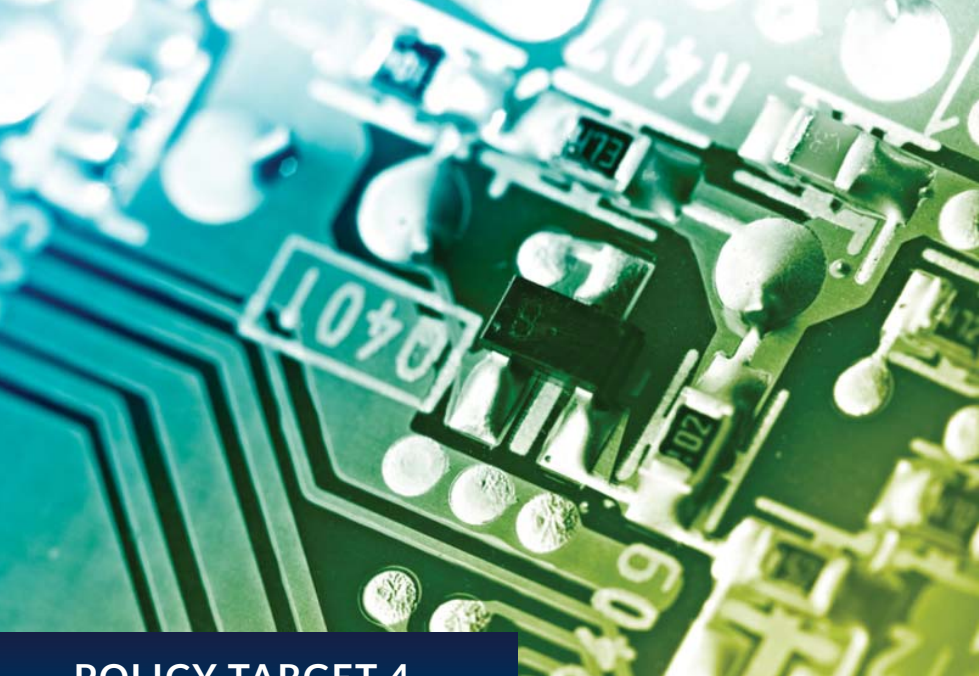
Action #2 |

Facilitating reporting and establishing or supporting hotlines.

Many member states, including Albania, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Portugal, Romania, Slovenia, the United Kingdom and the United States, reported newly established, or expanded use of existing, hotlines dedicated to the reporting of suspected online child sexual abuse. Moreover, a number of states reported ongoing participation in the IN-HOPE network. Spain provides model Memoranda of Understanding between law enforcement, hotlines and ISPs, with the aim of avoiding gaps in coverage, eliminating bottlenecks in information flow, and ensuring effective preservation of evidence for investigations. In addition to encouraging domestic reporting, the United Kingdom noted that it is working to share its expertise with smaller or developing countries that do not yet have a hotline, to facilitate more expansive reporting of online child pornography in those nations. In Denmark, Save the Children ran a campaign targeting human resource managers in 98 local municipalities encouraging reporting to the Danish national hotline of child pornography discovered on workplace servers.

Many member states reported newly established, or expanded use of existing, hotlines dedicated to the reporting of suspected online child sexual abuse. Moreover, a number of states reported ongoing participation in the INHOPE network.
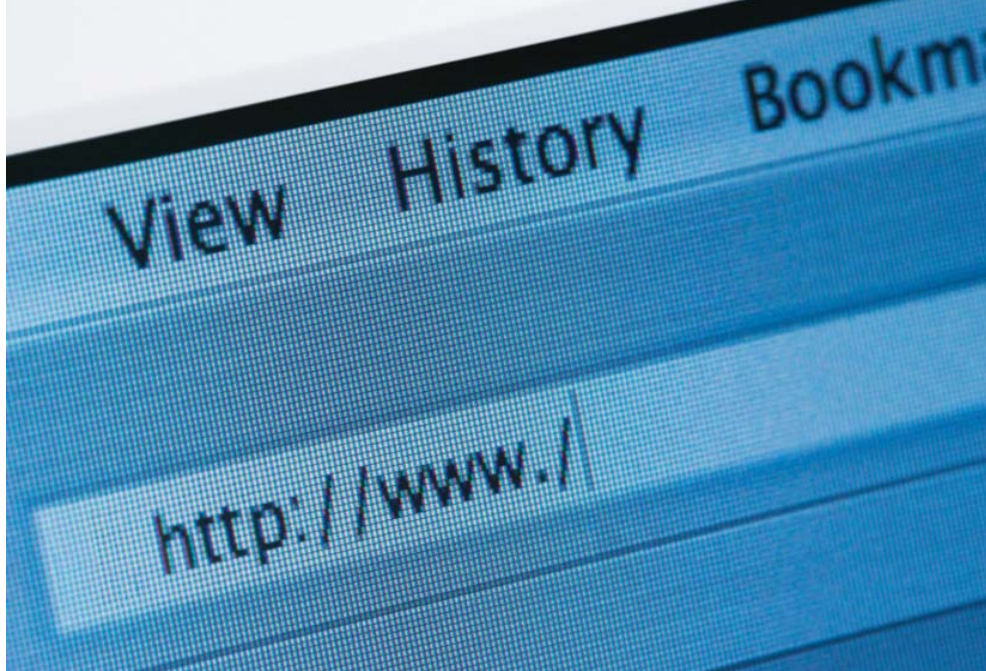
Action #3 |

Providing for the appropriate legal framework for notice and takedown procedures.

Most member states reported regular collaboration, through either formal or informal mechanisms, with ISPs to expedite the removal of child pornography hosted on domestic servers. Several states recently enacted new legislation to formalize those obligations. For example, Hungary's Internet Child Protection Act of 2013 extended the rules of notice and takedown procedures – previously limited to violations of intellectual property rights – to include violations of privacy rights of minors to expedite the removal of child pornography from the Internet. Cyprus enacted legislation that creates a legal obligation for ISPs to restrict access to websites containing child pornography, even in lieu of a court order, if they are informed by a competent authority (or otherwise obtain independent knowledge) of child pornography hosted on those websites. In Italy, ISP failure to cooperate with notice and takedown legislation, results in a fine of between 50,000 and 250,000 euros. In 2014, Israel enacted legislation enabling the police to instruct ISPs to block access to portions, or the entirety, of a website that supports the commission of certain offenses, including hosting child pornography.

Most member states reported regular collaboration, through either formal or informal mechanisms, with ISPs to expedite the removal of child pornography hosted on domestic servers.

Action #4 |

Removing and disabling access to child sexual abuse images.

A number of member states reported the implementation of successful blocking or filtering schemes, either legally mandated or voluntary on the part of ISPs, including Bulgaria, Cyprus, Ireland, Israel, Italy, Japan, Malta, the Netherlands, New Zealand, and Norway. In 2014, Bulgaria established a pilot program with five of its largest ISPs, in which those providers agreed to block access for all users to domain addresses known to contain materials involving the sexual exploitation of children. Japan collaborated with mobile phone carriers to develop customizable mobile phone filtering services, designed to block access to contraband materials and sites. Beginning in the spring of 2014, Japanese mobile phone carriers announced that they would carefully explain and promote filtering services when contracting with minors purchasing mobile devices or mobile contracts. Mexico passed legislation mandating that ISPs make parental restriction services available upon user request, which has dramatically increased parental awareness of Internet-facilitated child sexual abuse.

> A number of member states reported the implementation of successful blocking or filtering schemes, either legally mandated or voluntary on the part of ISPs.

Conclusion

The online sexual exploitation of children continues to pose a grave challenge to nations around the world. Since the inception of the Global Alliance, technological advances have emboldened offenders to an unprecedented degree. Cloud storage, for example, enables offenders to easily and cheaply store tens of thousands of images or videos outside of a residence or place of business, and access those files from anywhere in the world. Encryption prevents even the most technically-proficient investigators from accessing contraband materials. Anonymizing technology thwarts traditionally successful investigative techniques for locating offenders, creating a safe haven where offenders can act with impunity. Innovations in mobile technology, especially those that enable the easy and anonymous production and sharing of videos, allow offenders to entice naive and trusting minors to more readily share self-produced explicit images via the Internet.

Fortunately, as reflected by the Progress Reports submitted by Global Alliance members, technology also has the potential to revolutionize and enhance our collective abilities to prevent, detect, and disrupt online child sexual abuse and exploitation and to identify and prosecute of-

fenders. For example, we employ technology to engage and educate minors susceptible to exploitation where, increasingly, that exploitation first occurs -- on the Internet, on social media, and on mobile technologies. Collaborative technology enables more efficient identification of minor victims, and we continue to expand our international database of child pornography images in the hope that one day, no victim of an online child exploitation offense will ever be anonymous. We also employ novel investigative techniques to counter the increasingly sophisticated tactics used by offenders to obscure their identities.

In addition, Global Alliance members have addressed some of the jurisdictional challenges posed by multinational investigations into what is increasingly a borderless crime. Continued international cooperation and collaboration will ensure that no offender is able to escape liability by operating out of a jurisdiction with a more permissive legal regime.

The broad policy measures embraced by the Global Alliance over the past two years will help each and every child at risk, as well as each previously-exploited child who lives in fear of further dissemination of recorded abuse. And it is crucial for us to continue, and expand upon, our unrelenting efforts to forcefully respond to the epidemic of child sexual abuse online.