

# Global Research Project:

A Global Landscape of Hotlines Combating Child Sexual Abuse  
Material on the Internet and an Assessment of Shared Challenges





# Global Research Project:

A Global Landscape of Hotlines Combating Child Sexual Abuse Material on  
the Internet and an Assessment of Shared Challenges

Melissa Stroebel

Project Manager, Exploited Children Division  
National Center for Missing & Exploited Children

Stacy Jeleniewski, PhD

Research Analyst, Exploited Children Division  
National Center for Missing & Exploited Children



## About the National Center for Missing & Exploited Children

The National Center for Missing & Exploited Children® was established in 1984 as a private, nonprofit 501(c)(3) organization to help find missing children, reduce child sexual exploitation and prevent child victimization. NCMEC has created a unique public and private partnership to build a coordinated, national response to the problem of missing and sexually exploited children, establish a missing children hotline and serve as the national clearinghouse for information related to these issues.

Over the last 31 years, our national toll-free hotline, 1-800-THE-LOST® (1-800-843-5678), has handled more than 4 million calls. With help from corporate partners, we have circulated billions of photos of missing children and assisted families and law enforcement in the recovery of more than 216,000 missing children.

NCMEC also operates the CyberTipline®, a national mechanism for the public and electronic service providers to report suspected child pornography, child sex trafficking and other forms of child sexual exploitation. Since 1998, the CyberTipline has received more than 6 million reports of suspected child sexual exploitation, and since 2002, NCMEC's Child Victim Identification Program has reviewed more than 149 million suspected child pornography image and video files.

Since launching our first safety programs more than two decades ago, we have worked to put in place the policies, educational initiatives and public-private partnerships to prevent the victimization of children. That work continues today through our KidSmartz™ program, NetSmartz® Workshop, Technology Coalition, Financial Coalition Against Child Pornography and other initiatives to confront ever-changing risks to the safety of our children.

To learn more about NCMEC, visit [www.missingkids.org](http://www.missingkids.org).



## About Google.org

Google.org, the philanthropic arm of Google, was created to invent, experiment, and iterate on ideas to help make the world a better place using technology. Google.org develops and invests in people and ideas that can help bring shared knowledge to local, regional and global issues around poverty alleviation, public health, access to education and more.

For more information, visit [www.google.org](http://www.google.org).

# Contents

Acknowledgments.....	11
Letter from the NCMEC CEO.....	12
Executive Summary .....	15
Methodology.....	19
Global Landscape .....	21
Shared Challenges .....	31
Looking Ahead .....	39
Final Remarks.....	44
Appendix: Hotline Profiles.....	47



# Acknowledgments

The National Center For Missing & Exploited Children® wishes to thank the many organizations and people who have contributed to this project.

This report was made possible through the financial support of Google.org. A special thank you to Google team members: Chris Busselle, Justin Kosslyn and Sarah Holland for their unwavering support and guidance through this project.

We would also like to recognize the INHOPE Secretariat and its current Board of Directors, for supporting our collaboration with its membership and offering a forum to provide regular updates.

Lastly, our thanks to the hotlines around the globe combating online Child Sexual Abuse Material, who made time to respond to our many inquiries. The level of insight gained through this project was only possible because of their participation:

- *ACMA (Australia)*
- *AFA - pointdecontact.net (France)*
- *APLE Cambodia (Cambodia)*
- *ARC Fund (Bulgaria)*
- *ASI Mexico (Mexico)*
- *Barnaheill (Iceland)*
- *Be Smart Online - Aġenzija Appoġġ (Malta)*
- *Biztonsagosinternet Hotline (Hungary)*
- *Child Focus (Belgium)*
- *CNTI (Cyprus)*
- *CNZD (Croatia)*
- *Communications Regulatory Authority of the Republic of Lithuania (Lithuania)*
- *Consejo Ciudadano de DF (Mexico)*
- *cybertip.ca (Canada)*
- *CyberTipline (United States of America)*
- *ECO (Germany)*
- *ECPAT (Sweden)*
- *Emmaus - International Forum of Solidarity (Bosnia & Herzegovina)*
- *eSlovensko (Slovakia)*
- *Estonian Union for Child Welfare (Estonia)*
- *FCCN - Linha Alerta (Portugal)*
- *Film Publication Board (South Africa)*
- *Friendly Runet Foundation (Russia)*
- *FSM (Germany)*
- *Horka linka (Czech Republic)*
- *ICTA (Turkey)*
- *Internet Association Japan (Japan)*
- *Internet Association of Kazakhstan (Kazakhstan)*
- *Internet Foundation for the Development of Thailand (Thailand)*
- *Internet Hotline (Hungary)*
- *Internet Watch Foundation (United Kingdom)*
- *ISPAI (Ireland)*
- *jugendschutz.net (Germany)*
- *Korean Communications Standards Commission (Korea)*
- *Latvian Internet Association - Net Safe (Latvia)*
- *LISA Stopleveline (Luxembourg)*
- *Meldpunt (Netherlands)*
- *NASK / Dyżurnet.pl (Poland)*
- *National Internet-Safety Node in Russia (Russia)*
- *Net Patrola (Serbia)*
- *Netsafe (New Zealand)*
- *Red Barnet (Denmark)*
- *Red Peruana contra la Pornografia Infantil (Peru)*
- *SafeNet (Greece)*
- *Safernet.ro (Romania)*
- *Spletno Oko (Slovenia)*
- *Save the Children (Finland)*
- *Save the Children (Italy)*
- *Stopleveline (Austria)*
- *Të Protejo (Colombia)*
- *Telefono Azzurro (Italy)*
- *Web547 (Taiwan)*

## Letter from the NCMEC CEO

As acting chief executive officer of The National Center for Missing & Exploited Children, I'm reminded daily of the harmful and devastating impact of child sexual exploitation. NCMEC was created as a private, non-profit organization in 1984. NCMEC operates as the national clearinghouse and is designated by the U.S. Congress to receive federal funds to work on issues related to missing and exploited children. Our organization provides services to families, private industry, law enforcement, victims and the general public to assist in the prevention of child abductions, the recovery of missing children and the provision of services to combat child sexual exploitation. Since 1998, our CyberTipline has received more than 6 million reports regarding suspected child sexual exploitation and since 2002, our Child Victim Identification Program has reviewed more than 149 million suspected child sexual abuse images and videos.

Our experience indicates that the number of images being collected and traded by offenders worldwide continues to expand exponentially, and these images include graphic and violent abuse and feature young children, including infants. Despite criminal and civil efforts to stem its tide, child sexual abuse material remains a pervasive and growing problem.

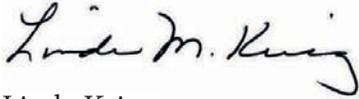
In recent years, the demand for and trade of child sexual abuse images has been increasingly facilitated by technological advances, including the increased use of digital recording devices, more storage capacity and faster Internet speeds. The ready availability of digital cameras (with no need for an outside photo developer), recording devices and smart phones has facilitated the creation of new child sexual abuse images and videos, while increased storage capacity and faster Internet speeds have permitted offenders to view and share larger numbers of photos and videos—with some offenders having collections containing tens of thousands of images and videos. In particular, the growing popularity of “peer-to-peer” file sharing, which permits direct, anonymous file-sharing between two or more users without cost to either user, has made distribution a common aspect of child pornography offenses. Collectively, these technological changes have facilitated offenders' ability to create, possess and distribute ever-larger volumes of child pornography.

Technology is, and will continue to be, an integral tool in the effort to disrupt online child sexual abuse material. Technology alone, however, cannot be our only tool. Effective partnerships with NGOs, law enforcement, industry and the public play a vital role in protecting our children from sexual abuse.

I'm pleased with the robust hotline participation and findings/recommendations from the Global Research Project, funded by Google. This report highlights some of challenges in the hotline community from a technical, legal and operational aspect. The report goes further to

recommend how organizations can better partner, embrace technology, streamline workflows and ultimately enhance the global response to this pervasive issue.

I'd like to recognize and thank Google for its unwavering commitment and support, not only for this project, but for all of its efforts in advancing technology in the protection of children online.

A handwritten signature in black ink that reads "Linda M. Krieg". The signature is written in a cursive style with a large initial "L" and a distinct "K" at the end.

Linda Krieg,  
NCMEC Acting CEO





## Executive Summary

Conducted by the National Center for Missing & Exploited Children® and funded by Google.org, the Global Research Project was an examination of hotlines combating Internet-facilitated Child Sexual Abuse Material.<sup>1</sup> The online sexual exploitation of children is a global challenge and countries around the world are uniting in pursuit of a comprehensive plan to prevent and disrupt the online spread of CSAM. By conducting this research, NCMCEC hopes to create a better understanding of the current global response to CSAM, the challenges hotlines encounter and most specifically, how community focused technology advances can increase hotline impact.

### The Research

Fifty-two hotlines participated by completing an online survey and follow-up interview. Research questions focused on four central themes: each hotline’s legal, technical and operational frameworks and community challenges. Findings of this research have been synthesized into a Global Landscape – outlining the operational, legal and technological workings of organizations combating Internet-based CSAM; Shared Challenges – examining the leading pain points

---

<sup>1</sup> For the purposes of this report, the term “child sexual abuse material,” or CSAM, will generally be used to describe any visual content depicting sexual acts involving a minor. Similar terms include child pornography and child sexual abuse images.

facing the community; and Looking Ahead – a forward-looking discussion of action items to address challenges underscored by this research.

## Global Landscape

Hotlines combating CSAM were located in 48 countries. While these hotlines recognize the importance of collaboration and actively partner through global membership organizations such as INHOPE, there are almost 150 countries where no CSAM hotline service could be identified.

In examining the operational, legal, and technological capabilities of these global hotlines, both similarities and differences were identified. While hotlines varied in several areas including organization size, funding sources and report volume, numerous important similarities exist which can inform community focused technology development.

Most hotlines identify as non-profit organizations that collaborate with stakeholders from many backgrounds, including law enforcement, the Internet industry and community-related groups. Though multi-stakeholder organizations, a large portion (67 percent) of hotlines are limited to either one or two funding sources. Ninety-six percent of organizations offer services in addition to the hotline and 85 percent accept hotline report types in addition to CSAM. Of those hotlines viewing CSAM, most (86 percent) offer services in support of staff well-being.

Additional differences and similarities were noted surrounding hotline technology infrastructure. First, each hotline has a distinct system for operations, frequently built using two or more pieced together, off-the-shelf systems. Second, although many hotlines (64 percent) use organization personnel for technology maintenance and development, these staff are generally shared across a larger organization, are limited in numbers and at times are actually hotline analysts serving a dual purpose.

## Shared Challenges

Based on the findings of the online survey and follow-up interview, five core areas emerged as hotlines' primary shared operational and technological challenges.

**Hotline administrators mentioned a variety of issue-based challenges stemming from the nature of their work combating CSAM online.** Most commonly, hotline administrators mentioned an increase in grooming<sup>2</sup> on social networking sites, a rise in complaints regarding

---

<sup>2</sup> Online grooming is commonly defined as a process in which an offender attempts to establish a relationship with a child in order to develop a sexual relationship.

the dark web<sup>3</sup> and anonymizing services and an increase in the length and number of CSAM videos.

**Many hotline administrators shared challenges regarding their collaboration with Electronic Service Providers<sup>4</sup>.** While it's common for some leaders of industry to proactively take steps to eliminate CSAM on their servers, in other cases, ESPs are not aware of how their system can be exploited or how they can take proactive steps to combat this exploitation. As a result, hotlines must rely heavily on personal outreach to build understanding of the issue within the ESP community.

**Hotline administrators commonly shared issues related to funding.** For most hotlines, funding can be unpredictable and, at times, insufficient. Irrespective of how long an organization has been operational, their size or their volume of reports, hotlines' capabilities are strongly impacted by funding concerns. In regard to technological capabilities specifically, this often results in hotlines investing in technological improvements as a reaction to a pressing need rather than as a proactive measure to plan for the future.

**Hotline administrators frequently commented on the need for increased automation and integration in some aspect or capacity.** At both the local and global levels, the hotline community remains heavily reliant on manual operations, resulting in strong interest across the community in new case management tools that would offer increased automation and/or integration.

**Hotline administrators commonly shared the view that the international response to CSAM online is fractured or disjointed.** The availability and operations of hotlines around the world seems to be largely impacted by global policy, cultural and legal differences, and economic challenges. Globally, only 54 hotlines operated by 48 countries could be identified as combating Internet facilitated CSAM. Of those hotlines, their missions and global contributions vary based on each country's policies, and international collaboration is frequently hindered by these differences. As a result, there can be duplication of effort and slower investigations.

## Looking Ahead

In the future, the hotline community would greatly benefit from technological solutions that address these shared challenges. In determining what solutions would be most beneficial, several criteria were considered, including the significance of the issue to hotlines, the potential impact on combating CSAM, and the technical complexity.

---

3 According to Andy Greenberg, the dark web is a collection of websites using anonymity tools like TOR and I2P to hide the IP address ("Hacker Lexicon: What Is the Dark Web? | WIRED," Andy Greenberg, accessed August 24, 2015, <http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>). While this area of the web is frequently used for criminal activity including drug sales and trade in child sexual abuse material, it also protects users such as political activists, whistleblowers, journalists and domestic violence survivors from surveillance and censorship ("Tor Challenge," Electronic Frontier Foundation, accessed March 19, 2015, <https://www.eff.org/torchallenge/>).

4 Electronic Service Provider (ESP) refers to any company offering services including but not limited to email, chat, and websites via computer, telephone, tablet etc. Similar terms include Internet Service Provider (ISP) and Information and Communications Technology (ICT).

Based on these criteria, the top two priorities for technology development were:

1. Process automation, with attention on integration with centralized databases, tracing tools, video analysis tools and CSAM URL notices and takedown.
2. Expanded data analytics, with attention on hotline level statistical solutions and global trend analysis.

To help implement any of the current, and future, technological solutions to the hotline community's shared challenges, it is recommended that a technology working group be established. Comprised of hotline representatives and technology experts, the technology working group could help develop and implement technological solutions and proactively monitor shifting technological trends in CSAM.

Technology plays a vital role in combating online CSAM; however efforts must stay relevant to both the issue and the needs of the organizations responding. Organizations must continue to monitor the shifting trends in exploitation and work to ensure those combating CSAM have the technological means to protect children from victimization.

## Methodology

The Global Research Project was a one-year research initiative by the National Center for Missing & Exploited Children made possible through the financial support of Google.org. Fifty-four hotlines combating CSAM online were invited to participate in the current project. Of those hotlines invited, 52 were available to participate. Invitations were extended to any hotline that could be identified as responding to Internet-facilitated child sexual exploitation, irrespective of if the hotline services were fully operational or still in development.

Initially, hotline administrators were contacted by NCMCEC staff and provided with information about the goals and projected milestones of the project and detailed requirements of their participation. Their participation was voluntary and the hotlines were not compensated for their participation.

In the first phase of the project, hotline administrators were asked to complete an online survey which asked questions regarding their organization and their hotline, specifically focused on the following areas:

- Legal: What is the scope of the organization's work? Under what legal authorities does the organization work?
- Technical: What is the technical stack in use? What is the size and capabilities of the engineering staff?
- Operational: What are the organizational practices? How is the organization staffed? Who are the stakeholders? What processes take place when a report is received?
- Issues: What are the organization's pain points? What solutions are needed to streamline workflow and output? From the organization's viewpoint, what paths of action could most effectively combat global CSAM?

This survey included approximately 100 questions; however, the actual number of questions that hotline administrators answered varied depending on their responses. Hotlines were provided with the survey questions and were encouraged to collect the necessary information to complete the online survey before beginning.

At the completion of this first phase, survey data was analyzed and interpreted to identify major themes in their responses, particularly in regard to challenges shared across the hotline community. Based on these themes, a second phase of data collection was conducted to acquire more information about these challenges and included follow-up interviews via video chats or phone calls. Depending on the extent of the hotlines' report process, these interviews took

approximately 30-60 minutes to complete.

Lastly, after phase two of data collection was complete, hotlines' data was further analyzed for additional trends and shared challenges. Hotline administrators were re-contacted several weeks after the completion of the interviews and asked to review and approve the information included in their hotline's profile.

## Global Landscape

The online sexual exploitation of children is a global challenge and countries around the world are uniting to pursue a comprehensive plan to both prevent and disrupt the online spread of CSAM. To further this fight, it's important to understand both the current global response and the community of hotlines collaborating on this mission.

The global landscape focuses on key trends stemming from the legal, technical and operational framework of the global CSAM hotline community. In addition to a brief history of the international response to online CSAM and development of the International Association of Internet Hotlines, it will discuss trends in legal authorizations, hotline operations and technological infrastructure.

### Development of a Global Response

In June 1996, the first Internet hotline dealing with CSAM was established in the Netherlands. By the end of that year, similar initiatives followed in several European countries, ultimately leading to the development of an international forum in 1997. Funded by the European Commission's Daphne program, a non-profit organization aimed at promoting children's interests in international communications, this forum was developed in an attempt to enhance hotline communication and collaboration regarding CSAM issues. This forum would develop into what is now INHOPE.<sup>5</sup>

Established in 1999, INHOPE is an umbrella organization supporting a global network of hotlines which receive reports of suspected online child sexual abuse material. "Member" hotlines meet regularly to share knowledge and best practices, examine emerging trends, inform global policy development and support developing hotlines. In addition, members utilize a shared database to facilitate referral of reports to other member countries and contribute data to monitor global trends in child exploitation.<sup>6</sup>

In 2010, the INHOPE Foundation was created, a separate charitable organization with the goal of helping to develop new hotlines worldwide, particularly in countries in which there is a lack of funding and/or legislation.<sup>7</sup> The INHOPE Foundation supports emerging hotlines as they establish the basic hotline operations by providing technical expertise, best practices, training and facilitating contact with experienced hotlines. At the writing of this report, INHOPE

---

5 "At A Glance," INHOPE, accessed August 24, 2015, <http://www.inhope.org/gns/who-we-are/at-a-glance.aspx>.

6 "At A Glance."

7 "At A Glance."

reports 46 “Member” hotlines and six “Foundation” hotlines.

In addition to the INHOPE Foundation’s work to support developing hotlines, the UK’s Internet Watch Foundation launched its “International Reporting Solution” in 2014 as another route to increase global response to online CSAM. Per IWF,

“As establishing the operational capability of a hotline brings significant costs (offices, staff, training, a welfare program, ICT and ICT security, establishing national procedures and building international networks), the IWF offers the use of its existing hotline facilities to other countries so that they can provide a full hotline service to their citizens at a fraction of the cost of a full, independent hotline... In addition, the IWF will assist in setting up country-customized notice and takedown procedures for content found within that country’s territory and engage with local internet industry to help them protect their networks”<sup>8</sup>

While this tool may not deliver expanded services sometimes offered by independent hotlines, such as community specific Internet safety initiatives or direct victim services, it can be a very cost effective way for countries that are not equipped with a hotline to provide their citizens with a reporting mechanism for CSAM.

Only launched in 2014, this service is still in its infancy. At the writing of this report the service had been fully implemented in Mauritius and is being considered for several other countries

Examining all hotlines identified around the globe, irrespective of availability to participate in this study, 48 countries have hotline services. These countries span the majority of continents, including North America, Europe, Australia, South America, Asia and Africa. Despite growing interest and momentum in many countries and regions, there are still 149 countries worldwide that do not have hotlines combating Internet-facilitated CSAM. As seen in the graphic below, South America, Africa and Asia in particular have limited access to hotline services.

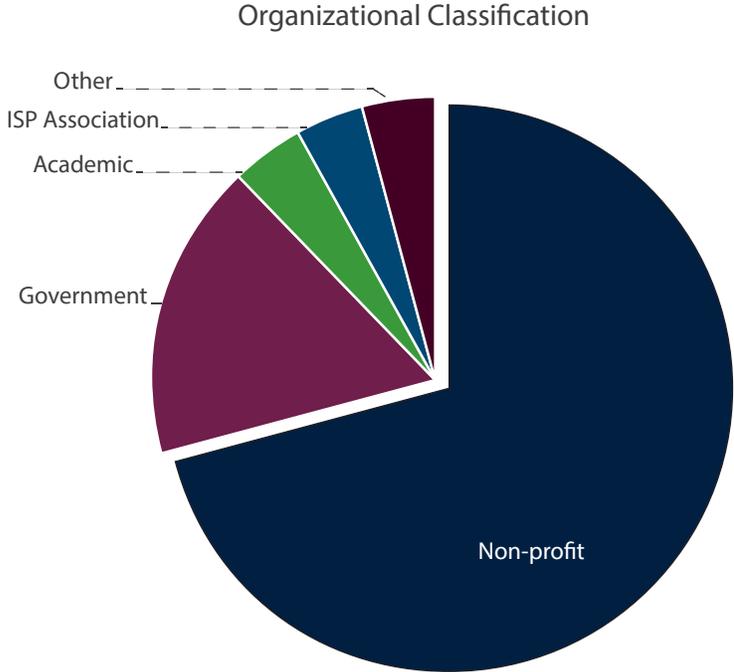
Global Hotline Availability



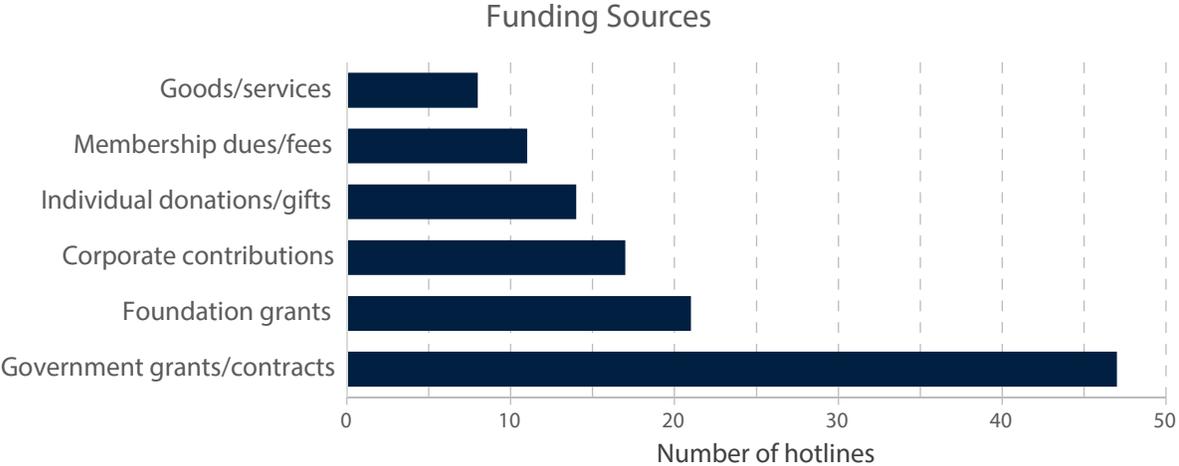
8 Chris Hughes (Hotline Manager, Internet Watch Foundation) in discussion with author, June 9, 2015.

### Organizational Structure

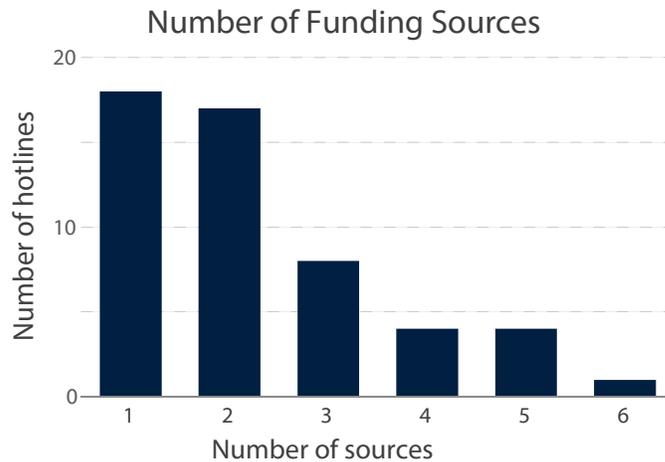
The majority of the organizations under which the hotlines function identify as non-profit organizations, followed by government organizations, academic institutions and ESP associations. Regardless of their identification, stakeholders for these hotlines span across many of these institutions and groups, including law enforcement, government, Internet service providers, social services, schools and the community.



Funding for the participating hotlines comes from a variety of sources. Although 90 percent of hotlines receive some degree of funding from government grants or contracts, hotlines also commonly receive funding from foundation grants (40 percent), corporate contributions (33 percent), individual donations/major gifts (27 percent), membership dues/fees (21 percent) and fees from goods/services (15 percent).

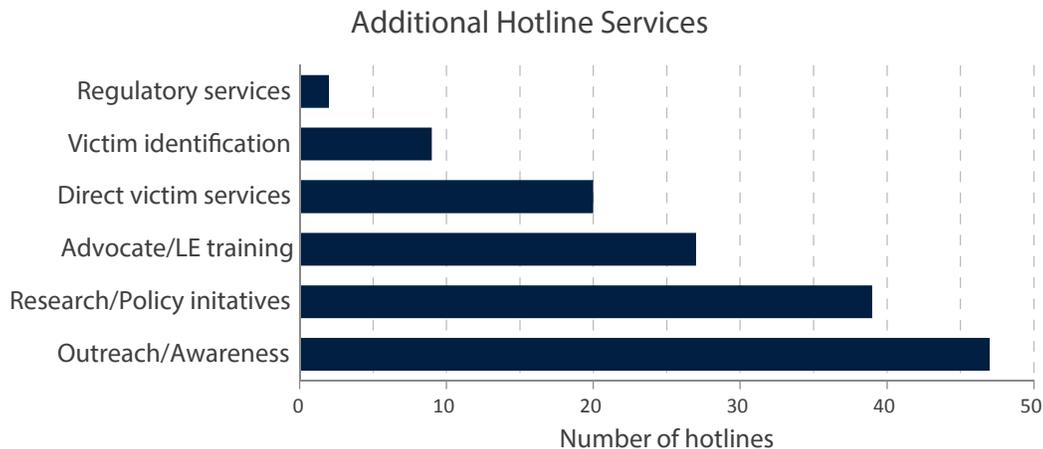


Approximately 67 percent of hotlines receive capital from only one or two of these funding categories. Some hotlines have more diversified funding pools and operate based on contributions from as many as six different types of sources.



There is great variety across hotlines regarding their organization’s size, primarily because some of the hotlines are the sole components of their organization while other hotlines are part of larger umbrella organizations. Nearly half (40 percent) of hotline administrators reported 10 or fewer staff and an additional 23 percent had between 10 and 50 staff. These small and moderately sized hotlines were primarily those that act as the sole component of their organization and are not part of a larger umbrella organization. In contrast, 19 percent of hotlines employ over 200 people.

Regardless of the size of these participating hotlines and their affiliated organizations, 96 percent offer services in addition to operating the hotline. The most common additional services included community outreach and Internet safety awareness, of which 90 percent of hotlines reported offering. For most organizations, these types of initiatives were not only reported to be one of the most common activities, but were viewed as core to the mission of their organization and an important tool for reducing child sexual abuse material online.



Beyond outreach and education, hotline administrators reported that their organization also engages in several other initiatives, such as research and/or policy initiatives (75 percent), advocate/law enforcement training (52 percent), direct services to victims (39 percent), victim identification (17 percent) and regulatory services (4 percent).

## Hotline Operations

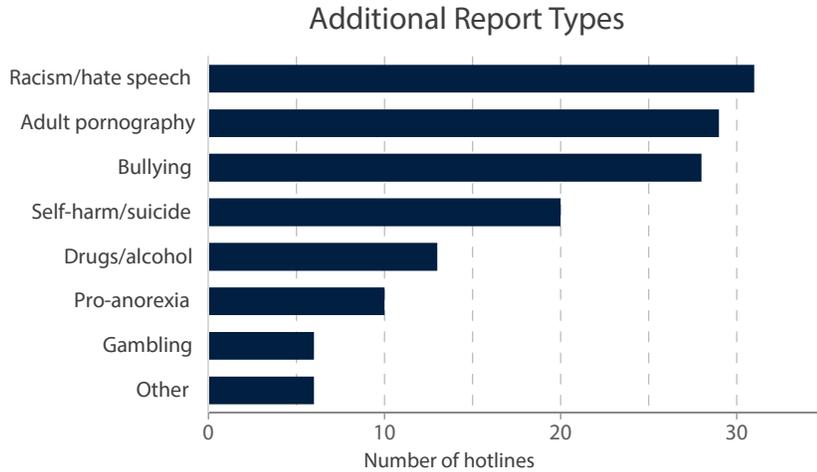
Hotlines participating in this survey have been in operation, on average, for nine years. However, the range of hotlines' years in operation varies greatly. While some hotlines have been in operation less than one full year, others have been in operation as long as 19 years.

Hotlines average three to four analysts processing CSAM reports. However, the number of years in operation appears to influence hotline staff size. Hotlines that have been in operation for less time have fewer analysts, and hotlines that have been in operation longer generally have more analysts. For example, no hotline in operation for less than five years has more than five analysts, and the two longest operating hotlines, at 17 and 19 years, have two of the highest number of hotline analysts, with 20 and 12 respectively.

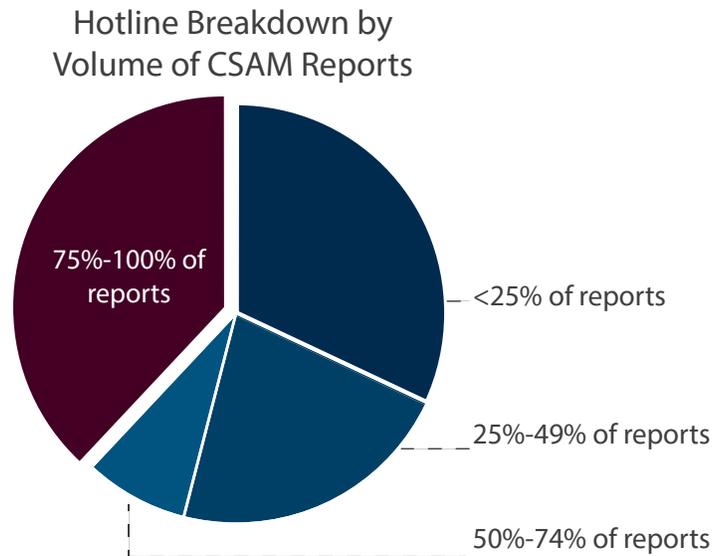
The number of reports received each year varies greatly across hotlines, from as few as 68 reports a year to more than 500,000 (in 2013). Despite this significant range, 50 percent of hotlines received fewer than 3,000 reports a year in 2013. It should be noted that several high volume hotlines are also in operation. During 2013, the four highest volume hotlines reported receiving 505,280 reports, 149,563 reports, 130,720 reports and 104,400 reports. Fortunately, the number of hotline staff tends to correlate to the number of reports that hotlines receive per year, and higher volume hotlines generally had more hotline staff.

Together, the number of reports received by the hotline and the number of staff used to analyze the reports help inform the average workload for an analyst each year. Examining these two factors in combination provides information concerning the general strain that analysts are under to complete their work. Hotline workload ranges significantly, from as few as 64 reports to 45,513 reports for each analyst each year at higher volume hotlines. Thirty-nine percent of responding hotlines show an individual workload of fewer than 1,000 reports each year, 47 percent reported 1,000 to 5,000 reports, 7 percent reported 5,001 to 10,000 reports and 7 percent reported greater than 10,000 reports.

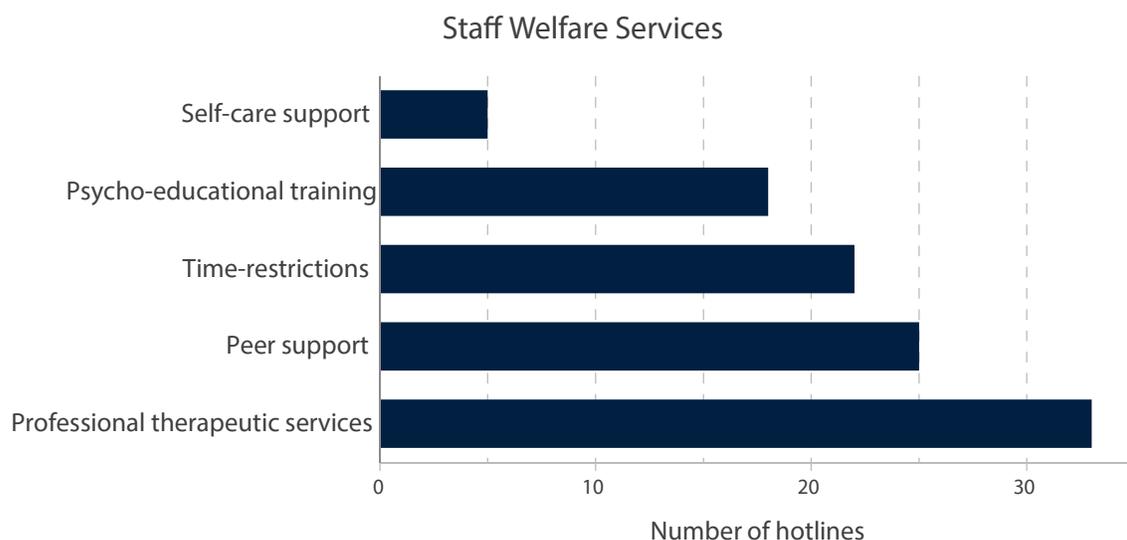
In addition to receiving reports regarding online CSAM, 85 percent of all hotlines also accept other report types, including, but not limited to, racism/hate speech (69 percent), adult pornography (64 percent), bullying (62 percent) and self-harm/suicide (44 percent).



While for the slight majority of hotlines reports regarding potential CSAM comprise less than half of their total reports, approximately one-third of hotlines surveyed indicated a workload in which the majority, if not all, reports relate to potential CSAM.



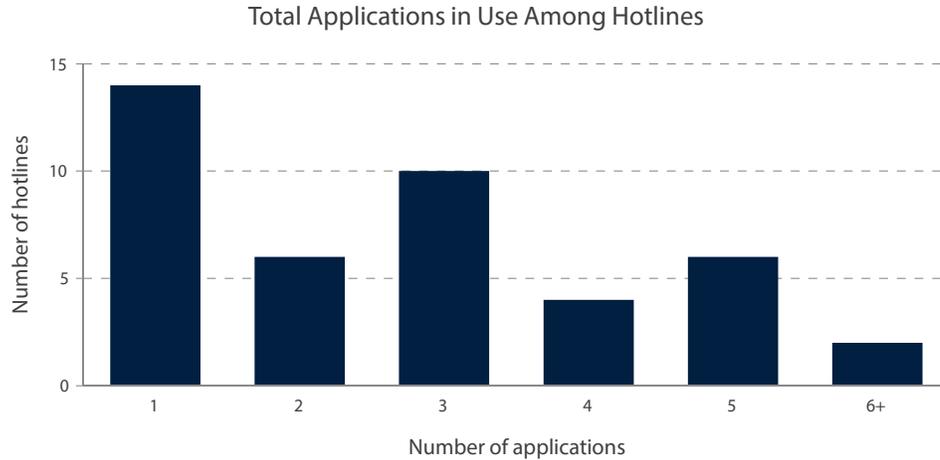
In consideration of the types of reports that hotline analysts are processing, the vast number of reports that many hotlines receive and the exposure of analysts to undeniably difficult content, staff welfare is a major priority to hotlines. Of those hotlines which view CSAM as part of their workflow, 86 percent offer services to support staff well-being. Hotlines offer a variety of services for this purpose including: professional therapeutic services, time-restrictions on analysts' exposure to CSAM, psycho-educational trainings, peer support and self-care support (e.g. gym membership).



## Technological Support and Infrastructure

Technological support and infrastructure are two of the most important factors in helping a hotline run smoothly. Impact is far reaching, whether it is regarding general computer and software maintenance, updating and maintaining the hotline's website and reporting mechanisms, or making complex upgrades to the case management system. Most hotlines (64 percent) reported that technological improvements are provided by in-house technology support, which was dedicated solely to the hotline, shared with their larger organization or contracted externally; 39 percent of these hotlines reported having only one person available for technology development and support. Regardless of the type of technological support, many hotlines reported that their analysts were also deeply involved in the technological development of the hotline due to limitations in the available technology support, often as a result of funding issues or workload-constraints. For some hotlines, their in-house technological support staff are actually hotline analysts playing dual roles as technology support.

In regard to technological infrastructure, two important factors emerged related to the managing and processing of reports: (1) the number of applications used and (2) the type of application used, whether off-the-shelf or built in-house. Overall, most responding hotlines reported using one to three total off-the-shelf and customized in-house applications, although hotlines reported using anywhere between one and 10 total applications. Furthermore, while 29 percent of responding hotlines reported using a combination of both types of applications to manage and process reports, 71 percent reported solely using one type or the other.



Similar to the pattern of overall applications used, the use of off-the-shelf specific applications also varies. Of the responding hotlines, 60 percent reported using some type of off-the-shelf application, either solely or in combination with in-house applications. On average, hotlines reported using approximately two off-the-shelf applications. While hotlines most commonly reported using one (24 percent), three (12 percent) or four (10 percent) off-the-shelf applications, some hotlines reported using more than four (17 percent).

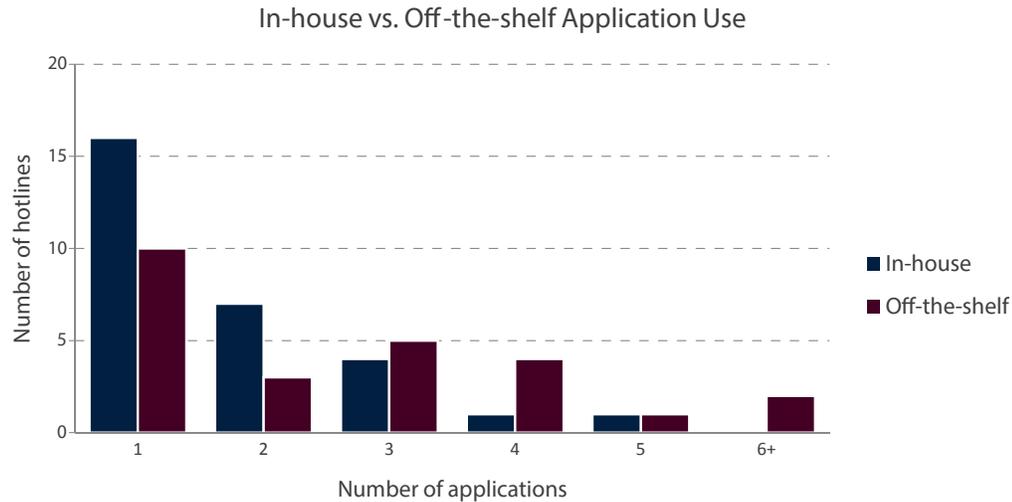
Among hotlines that reported using off-the-shelf applications, there was great variety in the applications used, particularly depending on the step of the reporting process. In receiving reports, all hotlines reported primarily using their customized web-based reporting form but a vast majority (81 percent) also reported using email in some capacity, whether it was to receive a report directly or used as a notification that a report was submitted using their web-based platform. To trace URL hosting locations, hotlines reported using CentralOps by far more than any other tool, followed by Firefox plug-ins/add-ons and RIPE. Many other less commonly reported tools include Robtex, ARIN, LAPNIC, JPNIC, IPNetInfo, Ping, Crimeflare, Maxmind, Wipmania, yougetsignal, visualiptrace and traceroute.

To access content, hotlines reported doing so via website browsers, although some hotlines specified using virtual machines and TOR-like proxies. Other tools hotlines reported using to access content included specialized tools, such as Shareaza or Transmission for peer-to-peer networks or Unison and newsreaders such as X-News for newsgroups. In watching videos specifically, hotlines most commonly reported using Windows Media Player and VLC media player.

Reports were forwarded to INHOPE affiliated hotlines primarily using INHOPE's Report Management System<sup>9</sup>. When notifying law enforcement, there was wide variation across hotlines, some of which specified using encrypted email or secure portal/virtual private networks while others reported using more basic approaches, such as providing printed documents. Lastly, hotlines reported primarily using email or phone to alert ESPs to CSAM hosted on their networks.

<sup>9</sup> The INHOPE Report Management System, or IHRMS, is used by INHOPE member hotlines to transfer reports of CSAM to other hotlines within the network.

In contrast to the use of off-the-shelf applications, a greater percentage of responding hotlines reported using applications that were built in-house (69 percent), either solely or in combination with some off-the-shelf applications. Most commonly, these hotlines reported using one (38 percent), two (17 percent) or three (10 percent) in-house applications while only 4 percent reported using four or five in-house applications. On average, however, hotlines reported using only one in-house application; a rate half that of off-the-shelf applications.



Among hotlines that reported using proprietary applications, there was great variety in the technological infrastructure used to deliver them. In regard to application and web-servers, the most commonly utilized are Apache and Windows servers. Other servers that hotlines reported using include Microsoft IIS, Typo3, PHP, GoDaddy, Linux and virtual servers. In contrast to this variety of servers for in-house applications, there was less variation in application databases and operating systems. More than any other database, reporting hotlines using in-house applications primarily reported using MySQL (79 percent), followed distantly by only 7 percent of reporting hotlines that use tailored versions of Microsoft Access. Similarly, there was also little variation in the operating systems reported to deliver these in-house applications, with Linux or Windows being the most commonly reported.

In regard to both the number and type of applications used, an important relation emerged between the two, such that, the number of applications that hotlines reported using is directly related to whether those applications are likely to be off-the-shelf or built in-house. More specifically, of the 14 hotlines that reported only using one application, the vast majority (86 percent) reported that the application was built in-house. In contrast, of those same hotlines, only 14 percent reported that that one application used was off-the-shelf. Furthermore, of the 12 hotlines that use more than the average number of applications, 92 percent reported using off-the-shelf applications while only 58 percent reported using in-house applications.

Overall, those hotlines that primarily use applications that are built in-house needed fewer applications to manage and process reports because the applications were designed to meet the specific needs of the hotline. In contrast, those hotlines that reported using more than

the average number of applications use a combination of off-the-shelf and built in-house applications, but are more likely to be using a greater number of off-the-shelf applications. Ultimately, hotlines may need fewer applications when those applications are tailored to their specific needs, whereas it may be a necessity to utilize a greater number of applications when those applications are purchased off-the-shelf.

## Global Landscape in Review

Based on the global landscape of hotlines combating CSAM, it is apparent that significant variation exists across hotlines regarding many factors, including organization size, funding sources, hotline staff size and in report volume. In addition, the tools and technology used to manage and process reports varies within hotlines processes, based on the step in the reporting process, and also across hotlines. Some hotlines use more off-the-shelf applications, while others have the ability to develop tailored applications that are built in-house.

Despite these differences, many similarities exist. Most hotlines identify as non-profit organizations that collaborate with stakeholders from many backgrounds, including law enforcement, the Internet industry and many community-related groups. In addition, most hotlines fall in the middle, between start-up hotlines that have been in operation less than a few years and whose report numbers are relatively low, and the extensively developed hotlines that have been in operation for over a decade and receive hundreds of thousands of reports.

Furthermore, and perhaps most importantly, hotlines share many of the same challenges, especially regarding funding and technological support, despite their vast differences. It's important to understand these shared challenges to appropriately identify and develop relevant solutions.

## Shared Challenges

In examining the survey data, several realities about the nature of CSAM and the current response were underscored:

1. While child sexual abuse material has always been a transnational issue, the central role held by the Internet in modern CSAM production and distribution demands an integrated and comprehensive global response.
2. Differences in regional policies, culture and resources present hurdles to this global response.
3. Though hotline remit, operational practices and resources vary, their common goal to disrupt the distribution of online CSAM presents many shared challenges.

The shared challenges identified through this report revolve around five core concerns: issue-based challenges, resources, collaboration with ESPs and the communication industries, existing technology infrastructures and a fractured international response.

### Issue-Based Challenges

The Internet is an ever-evolving community and provides immense opportunity for exploration and invention. However, this dynamic platform also presents challenges to those combating the production and spread of CSAM. While contending with analytical limitations tied to resources and operational guidelines, protection responses must keep up with shifting technology trends for each age group of children and the methods used by offenders to exploit them.

In survey interviews, 80 percent of responding hotlines remarked that they were seeing an increase in the use of social networking for child exploitation – either as a forum for grooming or as a source of self-generated, sexually explicit images of children. A 2013 report by the UK's Child Exploitation and Online Protection Centre noted several interesting statistics regarding juvenile behavior in regards to social networking:<sup>10</sup>

- Where it could be determined, CEOP found that social networking was the most prevalent offending platform for grooming at 49 percent, followed by instant messaging and chat.
- 13 – 14 year olds made up the largest group of victims at 35 percent; 11-12 year olds made up the next largest group at 22 percent.
- One quarter of social networking users age 8-11, and one third of users age 12-15,

---

<sup>10</sup> Statistics reflect year 2012 reports.

communicate with someone only known to them through the Internet.<sup>11</sup>

Hotlines also reported seeing an increasing number of complaints concerning illegal content hosted in areas such as dark web, cyberlockers<sup>12</sup> and content delivery networks,<sup>13</sup> 40 percent of hotlines specifically cite these systems as a source of added difficulty in analyzing reports. Offenders exploit these systems for numerous reasons including a perceived increase in anonymity, an opportunity to monetize their production and distribution of CSAM, and access to invitation only groups of offenders producing and trading new material. For 85 percent of hotlines participating in survey interviews, offenders' use of systems to hide their identity and/or location (e.g., TOR or proxy servers) was a significant problem. In addition, 41 percent of hotlines reported facing challenges with inconclusive trace results caused by fast flux domains<sup>14</sup> or diffused company holdings across country lines. Twenty-nine percent stated they were forwarded a report incorrectly as a result of such trace challenges.

Finally, evolving video software and faster Internet speeds are contributing to both the increased length and number of videos depicting the sexual abuse of children. Based on survey responses, 79 percent of hotlines reported the review of CSAM videos as a significant operational challenge for the following reasons:

1. The size of video files and hosting source can result in exceedingly long download times.
2. The manual review frequently needed to analyze video files is time consuming and mentally taxing for analysts.

Many file hosting sites exploited for distributing CSAM use premium accounts and rewards programs. This structure limits access of non-paying, non-sharing users and can result in a financial return to those sharing illegal content.<sup>15</sup> As non-contributing users of the sites, hotlines are generally not eligible for this type of access. Without premium account rights, hotlines face limits to the number of downloads and purposefully slow download speeds.

In addition, the review of videos is still largely manual and the volume of video files received by hotlines appears to be increasing; for example, the Canadian hotline reported a 230 percent

---

11 Child Exploitation and Online Protection Centre. *Threat Assessment of Child Sexual Exploitation and Abuse*, Child Exploitation and Online Protection Centre, 2013, 11.

12 Cyberlockers refers generally to websites that store content uploaded by users. This can include cloud storage, peer-to-peer networks, and media sharing services ("cyberlocker Definition from PC Magazine Encyclopedia," Ziff Davis, LLC. PCMag Digital Group, accessed May 29, 2015, <http://www.pcmag.com/encyclopedia/term/63854/cyberlocker>).

13 Content Delivery Networks (CDNs) aim to improve content delivery speed and security by regularly caching static content and distributing servers around the world.

14 Fast flux refers to linking a single domain to hundreds or thousands of different IP addresses which change as rapidly as every few minutes. This technique is seen employed by a variety of cybercriminals, including child predators, to hide the origin of a cyber-attack or website hosting illegal content such as CSAM ("HOW FAST-FLUX SERVICE NETWORKS WORK | The Honeynet Project," Jamie Riden, accessed August 20, 2015, <http://www.honeynet.org/node/132>).

15 European Financial Coalition Against Commercial Sexual Exploitation of Children Online, *Strategic Assessment of Commercial Sexual Exploitation of Children Online; Update*, European Financial Coalition against Commercial Sexual Exploitation of Children Online, 2015, 14.

increase in the number of videos analyzed from 2013 to 2014.<sup>16</sup> To confirm a video as depicting CSAM, a hotline must view the footage. In some cases, the first apparent CSAM may not be seen in a film until 20 minutes or more into footage. As the number of video files reported to hotlines rises, this review process becomes increasingly taxing.

## Collaboration with Electronic Service Providers and the Communications Industry

The level of collaboration with Electronic Service Providers and the communications industry varies significantly between countries. In many cases, ESPs actively partner with hotlines to help disrupt online CSAM. According to survey responses, 90 percent of hotlines reported that the Internet and communications industries are stakeholders in the hotline; 40 percent of hotlines reported that their country legally requires ESPs to take action on apparent CSAM found on their servers; and two of the hotlines are dedicated ESP associations which operate hotlines for improved self-regulation.

Based on conversations with participating hotlines, many ESPs have evolved into active, committed partners in the fight against Internet-facilitated child sexual exploitation. Leaders within the industry take voluntary steps to proactively identify and eliminate child sexual exploitation on their servers. While not all companies voluntarily choose (or are able based on local legislation) to proactively search for CSAM, many provide “Report Abuse” buttons, collaborate through working groups such as the CEO coalition,<sup>17</sup> award research grants to hotlines and provide financial support to develop future methods of combating online CSAM.

There are thousands of ESPs in operation around the world and many are not cognizant of online child sexual exploitation or as involved in combating it. In some cases, ESPs are simply not aware of how their system can be exploited and proactive steps they can take to prevent further distribution. Often, it falls to the hotline to seek out ESPs and educate them on the nature of Internet-facilitated child sexual abuse and how they can help fight it.

Of hotlines reporting they notify ESPs of apparent CSAM on their servers, 84 percent rely on personal contact with the provider and another 10 percent use a combination of automated notification and personal contact. In survey interviews, these hotlines frequently highlighted that this level of personal interaction with the ESPs has been necessary to help facilitate expeditious removal of content.

---

16 Stephen Sauer (Systems Specialist, Cybertip.ca) in discussion with author, June 16, 2015.

17 “The CEO coalition, launched in December 2011, is a cooperative voluntary intervention designed to respond to emerging challenges arising from the diverse ways in which young Europeans go online” (“Self-regulation for a Better Internet for Kids | Digital Agenda for Europe | European Commission,” European Commission, accessed June 22, 2015, <http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids>).

Statistics show how these vital partnerships are helping to speed up URL removal.<sup>18</sup> According to INHOPE global statistics on European member hotlines, 93 percent of CSAM reported to content service providers in 2014 was removed in less than 72 hours. However, 5 percent took four to six days for removal, and 2 percent required seven or more days for removal.<sup>19</sup> This is up from 2013 data that showed only 80 percent of reported URLs were removed within 72 hours, 13 percent were moved in four to seven days, and 7 percent were still online seven days after notice was sent.<sup>20</sup> It should be noted that in some cases longer removal times are a result of law enforcement's investigative procedure rather than lack of response by an ESP.

The nature of Internet distribution of CSAM means any delay in content removal facilitates the continued viewing and proliferation of illegal content. This in turn leads to further victimization of the children depicted in traded CSAM and unwanted exposure for online users. Collaboration with ESPs is improving content removal rates; however, this remains an area for continued development.

## Resources

As discussed in the Global Landscape, 71 percent of hotlines participating in this survey operate as non-profit organizations. According to survey responses, funding generally stems from government grants and contracts (90 percent), foundation grants (40 percent), corporate financial and in-kind contributions (33 percent), and individual donations (27 percent). As a result, funding can be unpredictable and, at times, insufficient. Irrespective of how long an organization had been operational, size of the organization or volume of reports, hotlines reported that additional funding would help them better translate organizational vision into action. This challenge is universal in the hotline community and impacts operations, technology and staffing.

Of particular concern for this project is the technological impact of funding concerns. Responses indicate funding challenges can restrict purchases of new hardware and software, limit training opportunities and hinder effective competition to hire and maintain qualified technical staff. As a result, hotlines' technological improvements more commonly occur as a reaction to a pressing need (such as maintenance and repair of current systems) rather than as a proactive measure to plan for the future.

## Existing Technology Infrastructure

18 URL removal refers to the practice of taking down content determined to be illegal within a country's legal framework. Some countries do not have the legal means to compel full removal of CSAM, and instead rely on filtering and blocking technology to at least restrict access to the material. While blocking and filtering technology is available for private use, removal must be managed on the industry and national levels.

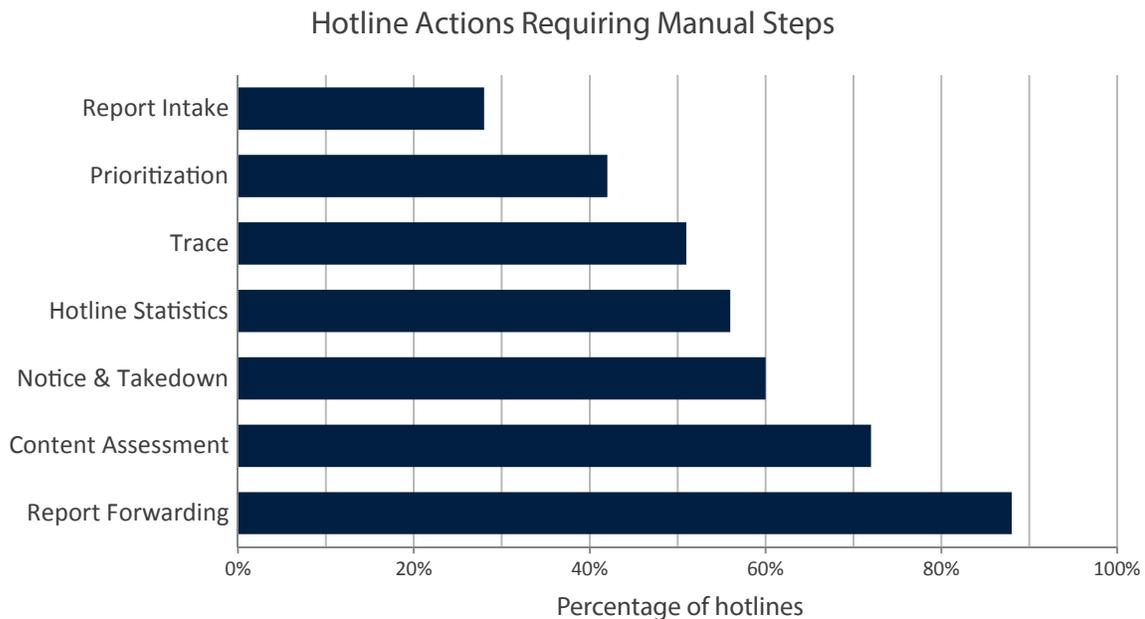
19 INHOPE, *INHOPE Stats Infographic for 2014*, INHOPE, 2015.

20 INHOPE, *2013 Infographic*, INHOPE, 2014.

Significant variation exists among hotlines in terms of internal technology infrastructure. Survey results indicate that hotline systems range along a spectrum from stand-alone, off-the-shelf programs to integrated, customized services built and maintained by in-house engineers. While some hotlines are developing forward-looking technology plans, most of the community’s operational practices remain reliant on manual operations. Given that hotlines without customized tools tend to use a greater number of unconnected off-the-shelf tools to meet their needs, the level of manual operations is especially relevant.

Hotline necessity and resources largely drive organizational technology and improvements, which rely heavily on the observations and recommendations of hotline analysts. In survey interviews, 72 percent of responding hotlines reported that in-house technology staff is available to improve hotline systems. Of those hotlines with in-house technical support, 52 percent rely on analysts to contribute to technology development. For example, two hotlines have no in-house technological support and rely solely on hotline analysts to play dual roles as both technological staff and analyst. Furthermore, 15 percent of the hotlines with in-house support still have to share technical staff with their larger organizations, thereby limiting availability for specific use by the hotline.

According to survey responses, hotlines operate largely through manual processes. While 94 percent of participating hotlines have access to some type of centralized report management system, 89 percent reported they were either somewhat or very interested in tools that would offer increased automation and system integration. Report intake was reported across hotlines as the most universally automated process. In contrast, information forwarding was reported as the step most reliant on analyst action.



Analyst expertise is not to be undervalued and is an integral component of hotline impact. For example, content assessment is one area where analyst input is vital. The human eye can quickly

and accurately identify finite visual clues in images and videos and staff experience informs a more tailored analysis targeted to case details. To maximize report processing capacity, technology must be utilized to ensure analyst time is reserved for the steps in which it can be most impactful.

A clear example of this is the review process for explicit images and videos. Two-thirds of participants in survey interviews reported they do not use hashing<sup>21</sup> to help review reported content. Incorporation of hashing technology could significantly reduce the time and effort spent on reviewing previously analyzed images. INHOPE reports approximately 6,000 of the websites catalogued in their report management system in 2014 were duplicates of previously reviewed material.<sup>22</sup> Eliminating re-review of this material can contribute to improved staff welfare and increased analyst availability for visually reviewing newly produced and distributed CSAM.

The hotline community recognizes the benefit of data sharing and collaboration. To enhance the exchange of information, hotlines are actively using technology to quickly disseminate information and share issue-based statistics. Currently, hotlines primarily rely on INHOPE's IHRMS for in-network URL referrals between hotlines. In addition, a developing system, known as IC-CAM,<sup>23</sup> aims to increase and enhance the use of hashing technology in content review. The project has completed a pilot period and is proceeding to the next phase of development and roll out within the European Union.

IHRMS is a good example of a technology which is positioned to significantly impact the global response to CSAM but may be hindered by a lack of effective integration with individual hotline systems. The system provides a framework for inter-agency collaboration through coordinating complaint referrals and monitoring of global CSAM trends. Unfortunately, differences in hotline operations and technology platforms make integration in a global system challenging. Under the current configuration, almost 90 percent of hotlines that reported contributions to these systems are reliant on manual analyst action and 82 percent found the contribution to be duplicative of work already completed in their hotline systems. The double entry of data from a hotline's database into the IHRMS absorbs analyst time and resources, which could be better focused elsewhere.

Finally, data analysis and reporting capabilities vary greatly between hotlines. When asked what areas technology could most improve their hotlines' processes, 66 percent of hotlines indicate the need for improved statistical capabilities. Accurate and accessible statistics are crucial for accurately forecasting staffing needs to keep up with workload, developing pertinent outreach

21 A hash value is a digital fingerprint unique to a particular image and based on a standard mathematical algorithm. Several different algorithms are in use, including MD5 and SHA (Federal Judicial Center, *Managing Discover of Electronic Information: A Pocket Guide for Judges*, by Barbara J. Rothstein, Ronald J. Hedges, and Elizabeth C. Wiggins, 2007, 24). If the photo is altered in any way – cropped, rotated, changed from color to black and white - the hash value is also altered.

22 *INHOPE Stats 2014*.

23 IC-CAM is a software solution aimed at limiting the re-review of CSAM by analysts and more effectively disrupting the spread of CSAM. The project, which was piloted with several hotlines in 2014, was funded by the European Commission and developed through partnership between INHOPE staff, member hotlines, Interpol and Dutch software vendor Zuiz (INSAFE & INHOPE, *BIKnet Matching Signatures (Hashes) Project 2014*, INSAFE & INHOPE, 2014, 3-4).

initiatives to prevent exploitation and cultivating funding sources to support hotline operations and future growth.

## Fractured International Response

An integrated and comprehensive global response is critical to effectively combating Internet-facilitated child sexual exploitation. The importance of this point cannot be overstated and has been underscored within the child protection community repeatedly over the last two decades. International efforts continue to strive for more uniform global standards for prevention, investigation and prosecution.

Cultural and legal differences, global policy and economic challenges impact the existence and operations of hotlines around the world. As mentioned in the Global Landscape section, hotlines combating Internet-facilitated CSAM could only be located in 48 countries.

Of those hotlines, their missions and global contributions are in part dependent on local policy. Despite significant efforts by hotlines to collaborate, data sharing and case deconfliction is frequently hindered by policy differences between countries. As a result, there can be duplication of effort, slower investigations and ultimately fewer children rescued.

The International Centre for Missing & Exploited Children<sup>24</sup> examines the variations in global policy closely in the report *Child Pornography: Model Legislation & Global Review*. The 7<sup>th</sup> edition of this report, published in 2012, examines challenges facing the global response to CSAM and the specific legislation of 196 countries around the globe.

The legislative review focused on five key components:

1. Does national legislation exist specific to CSAM?
2. Does the legislation define “child pornography?”
3. Does the legislation include use of a computer?
4. Does the legislation criminalize possession of CSAM regardless of intent to distribute?
5. Does the legislation require ESPs to report CSAM found on their networks?<sup>25</sup>

In terms of the global response to CSAM, perhaps the most significant issues surround the definition of child pornography and what constitutes a child. Legislation in some areas is broad and open to interpretation, while other countries identify specific acts which are criminalized.

---

24 The International Centre for Missing & Exploited Children, or ICMEC, empowers and equips global partners - in government, academia, law enforcement, private industry and the NGO community - to make the world a safer place for children by informing policy, training child protection officials, and promoting the creation of operational centers around the globe (“About ICMEC,” International Centre for Missing & Exploited Children, accessed July 15, 2015, [http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en\\_X1&PageId=1222](http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=1222)).

25 International Centre for Missing & Exploited Children. *Child Pornography: Model Legislation & Global Review, 7th edition*, International Centre for Missing & Exploited Children, 2013, 15.

The age of consent widely varies. According to UNICEF, in 2012 the age of consent ranges anywhere between 12 and 18 years of age depending on where you are, and in some countries the age limit varies between boys and girls.<sup>26</sup>

The concept of “dual criminality”<sup>27</sup> further complicates national prosecutions of this international violation. Countries may struggle to prosecute an offender for a crime committed overseas if both countries do not criminalize the act. Based on its review in 2012, ICMEC found 53 countries offered no legislation specifically addressing child pornography. Of those with legislation, 60 did not define child pornography and 47 did not criminalize possession regardless of intent to distribute.<sup>28</sup>

The challenge for individual hotlines around the world to know and understand the nuances of each country’s standards is momentous. As such, content which is not illegal in one country may not be referred to a hosting country where it is illegal, referrals may be made to a country that does not consider the material prohibited, and as a result, prosecutions may be limited due to these legislative conflicts.

Hotlines combating CSAM have taken the vital step of organizing global partnerships in the form of groups like INHOPE. However, these partnerships cannot singularly surmount the global policy inconsistencies and gaps in state supported response.

## Shared Challenges in Review

The survey of existing hotlines combating the production and spread of CSAM makes clear that though hotlines vary in mission, local policy, and resources, shared concerns exist and can be examined on the community level. In particular, the community is contending with challenges arising from the nature of online CSAM, ESP engagement, hotline resources, technological infrastructures, and a fractured global response. Moving ahead, this understanding should be leveraged to propel technological development for the hotline community.

---

26 “Are you old enough?” UNICEF, accessed August 24, 2015, [http://www.unicef.org/rightsite/433\\_457.htm#to\\_have\\_sex](http://www.unicef.org/rightsite/433_457.htm#to_have_sex).

27 Dual criminality refers to the need for an act to be illegal in both the country where the crime was committed and in the offender’s country in order for a prosecution to occur in the home country (*Child Pornography: Model Legislation*, 1).

28 *Child Pornography: Model Legislation*, iv.

## Looking Ahead

As previously stated, the focus of this project has been two-fold. First, to better understand the landscape of hotlines around the globe combating the production and dissemination of CSAM on the Internet. Second, to examine the challenges present in the community with a focus on identifying areas for which shared technological advances would be most beneficial.

The last section outlined a range of significant shared challenges within the hotline community. Moving forward, these issues must be prioritized to effectively assess and apply available resources. Researchers applied three core criteria in making this assessment: (1) significance of the issue to hotlines; (2) potential impact on combating CSAM; and (3) technical complexity. Several challenges and potential tools to address them were identified for further consideration:

Process automation, with attention on integration with centralized databases, tracing tools, video analysis tools, and CSAM URL notices and removal.

Expanded data analytics, with attention on hotline level statistical solutions and global trend analysis.

It should be noted that while we have a snapshot of challenges impacting the hotline community, it will be necessary to delve deeper into each issue, specifically examining user experience, legal and technical requirements to develop meaningful and high impact solutions.

### Process Automation

Responses throughout the survey show an unsustainable reliance on manual steps for hotline operations with more time spent on data collection and referral than data analysis. Given the limited staff size and increasing work load, improved automation will be critical for hotlines to keep up with the increasing number of reports and free up resources to expand services. In addition, for those hotlines with the legal authority to do so, increased automation could create opportunities for expanded focus toward identifying offenders and rescuing child victims.

Survey responses point to several areas where technology could improve process automation. These include, but are not limited to:

1. Database integration
2. URL notice and removal
3. Tracing
4. Video solutions

### *Database Integration*

A consistent concern throughout the hotline community is the lack of integration between core databases. This is true for both internal hotline systems within an organization and between global databases. The lack of integration results in duplication of work and an increased chance of data entry errors.

As previously mentioned, almost 90 percent of responding hotlines stated they would be either somewhat or very interested in an improved case management system. Further, 40 percent of hotline respondents specifically stated their system could be improved through increased integration within their internal systems. Workflow integration in hotline databases varied between hotlines and analytical processes. For example, while only 2 percent of hotlines do not have report intake built into their case management system, 45 percent of hotlines do not manage notice and removal records within their central database.

In addition to internal hotline services, increased integration of hotline systems with global databases would lead to improved information flow, increased efficiency and better global statistics.

INHOPE member hotlines utilize IHRMS as the conduit for report referral between countries. Because of the independent nature of each member hotline's development, the process of transferring reports from the local system to IHRMS is largely manual and can therefore be extremely time consuming, particularly for higher volume hotlines. Hotlines must enter all relevant report information – such as website URL, nature of content and host location – in order for the report to be forwarded to the hosting country. Furthermore, the hotline must re-access IHRMS to register when a CSAM website has been removed by the hosting provider. Failure to document the URL removal within the IHRMS in a timely fashion results in inaccurate data on content removal times.

Because the general report information has already been catalogued into the hotline database, this step is not only manual, but duplicates exact steps already completed by hotline analysts. There's an opportunity for saving significant staff resource time by eliminating the need to re-enter the same data into two different systems.

While enhancing global database integration will be challenging, and to an extent limited by variations between the 52 distinct hotline databases, development of a centralized database would greatly improve global flow of CSAM statistics to hotlines and stakeholders.

### *URL Notice and Removal*

Given the focus on disrupting circulation of CSAM online, hotlines must be able to securely, efficiently and accurately notify hosting providers when such material is found on the Internet. Most hotlines rely on a manual processes for ESP notification of illegal content and an ongoing manual review of webpages to verify the removal of content.

Hotlines recognize the importance of personal contact with ESPs, but technological tools can

automate portions of the notice and removal process without hindering the important step of industry outreach. For example, the process of physically notifying the hosting provider to the CSAM could be automated from within the hotline's database. As the analyst conducts their work, a message can be compiled based on data points and triggered by staff. This would eliminate reliance on analysts manually copying information from the database into an email to notify the providers. Increased automation can provide analysts more time to develop and maintain strong working relationships with ESPs. It could also streamline the receipt by the ESP as a notice could be sent from one hotline account versus multiple hotline analysts.

Some hotlines have already begun moving in this direction. For example, at the Canadian hotline Cybertip.ca, CSAM content on websites is hashed and the system automatically rechecks the page on regular increments to determine if the URL is still active and if the content on the page has changed. As a result, reported CSAM content is checked more frequently and analysts do not need to review previously assessed CSAM.

### *Tracing the Host Provider*

Hotlines that reported they attempt to trace the hosting location of CSAM content were also asked for additional detail on the workflow concerning this process. Of those hotlines responding, 45 percent reported this step is fully manual, including the copying the domain information from the hotline's system into a WHOIS tool, waiting for results, and copying the WHOIS results into the hotline's database. If a hotline processed hundreds of URLs in a day, this process can result in a considerable use of staff time and resources. An additional 37 percent of hotlines report the process is a combination of automated and manual actions. Further, 92 percent of hotlines reported challenges in identifying an accurate host location.

Hotlines use different tracing tools with varying results. Consistent feedback from the reporting hotlines is that host information is often inconclusive and requires additional review by an analyst using multiple tracing tools. Bundling a collection of trace tools into a single, automated hub could expedite the review and alert the analyst only if a discrepancy between trace tools occurs.

### *Video Solutions*

In survey interviews, 85 percent of hotlines reported viewing CSAM as part of their report assessment workflow and, of hotlines that view CSAM, 39 percent reported challenges with viewing videos. While some of these challenges stem from legal limitations, technological limitations were also commonly reported. More specifically, of those hotlines that can view videos and reported challenges in doing so, 18 percent indicated the challenges stemmed at least in part from manual review of video files, 18 percent found the review very time consuming, 16 percent experienced problems downloading the videos and 9 percent were confronted with increasingly long video files.

Furthermore, these technological limitations commonly occur in combination. Of the hotlines

that reported having issues viewing videos, 69 percent reported having two or more of these technological issues with viewing videos. Thus, if hotlines experience technological issues with viewing videos, it's more likely that they experience multiple limitations. Given the reliance on manual review of videos, it's unsurprising that other issues occur in combination; longer videos directly result in increased review times.

Exploring ways to add automation to the video review process may lessen the strain on analysts reviewing the material. For example, a system which flags scene changes within a video may expedite the review process and eliminate the need to view the full duration of the videos. Instead, analysts could quickly identify if the video has multiple scenes and advance through scenes to triage video content.

## Data Analytics

### *Local*

Data analysis is crucial for hotlines to identify shifting trends in child sexual exploitation, understand hotline workload as well as planning for future initiatives, such as organization expansion or prevention awareness messaging. Many hotlines report limited analytical tools for processing available information.

For example, although 90 percent of hotlines can extract data from a records management system, 61 percent of these hotlines must then manually analyze the information. Many hotlines report Microsoft Excel as their sole data analysis tool. While this is an effective program, expanding the hotline's resources for analysis would provide better data informed dialogues with ESPs, policy makers, funding sources and local communities.

### *Global*

The global nature of online child sexual exploitation demands a global understanding of both the issue and the response. This understanding cannot be limited to simply reporting on the issue, but must also make informed predictions based on shifting trends and discuss resources needed to address the problem.

Currently, INHOPE is the primary resource for such information. INHOPE members manually submit hotline statistics on a monthly basis to INHOPE. These updates allow INHOPE to capture the overall workload of a hotline and monitor evolving CSAM trends. On an annual basis, INHOPE uses this information to publish infographics that provide an overview of CSAM hosting, notice and removal, report origin and victim demographics for the previous year.

While these updates play an important part in informing policy and painting a picture of the successes achieved through INHOPE collaboration and the challenges facing its members, hotlines report this is an area that may benefit from improvement to enhance hotlines' processes of contributing and accessing data. For example, though informative, INHOPE's annual

infographics only provide a retrospective look. Furthermore, although contributing hotlines can access statistics submitted by their individual hotline, they cannot query the global data without assistance from INHOPE personnel.

Expanding INHOPE's data analytic capabilities can support increased trend forecasting and educate hotlines with awareness of global trends. The quickly shifting nature of online CSAM makes predictions challenging, but it is necessary to help hotlines respond to trends before they become outdated. Predictive reports will help individual hotlines and the entire community plan and prioritize technology development, staffing needs and outreach initiatives.

### Technology Working Group

Based on the results from this survey, it is recommended that a technology working group be established to monitor and advance technology development within the hotline community. The working group should consist of hotline representatives, INHOPE staff and technology experts.

In the immediate future, this working group could drill down on shared challenges highlighted through this survey. Hotline representatives could identify necessary requirements for effective hotline tools, and together with technology experts, be available to shape system design(s) according to needs outlined by hotlines.

The group could also discuss emerging challenges as they relate to developments in CSAM. Ideally, the group would function to proactively identify technology gaps and prioritize shared technology developments that can support hotlines when combating online CSAM.

### Looking Ahead in Review

Many shared challenges exist among the diverse community of hotlines combating global CSAM. Moving forward, it is vital to prioritize the challenges in an effort to maximize potential impact of shared solutions. A Technology Working Group can help to ensure immediate and future solutions and maximize available resources for protecting children.

## Final Remarks

This project provided a closer analysis concerning the availability and resources of hotlines combating online CSAM around the globe. Due in large part to the invaluable level of participation by these hotlines, this report is uniquely situated to offer direct insight into the legal, technical and operational capabilities of each organization and the shared challenges impacting the hotline community.

Hotlines play a vital role in the fight against online CSAM. They are bringing together members of the Internet industry, law enforcement, social services, policy makers and the public for a collective response to the issue. Hotlines are educating their communities about the realities of CSAM online and the significant and real harm caused to child victims by the distribution of each image. Collectively, these hotlines are arming millions with the knowledge and tools to disrupt the continued circulation of CSAM and prevent future victimization of children worldwide.

However, hotlines face significant challenges in their work, particularly in terms of mounting a unified international response to the global problem of CSAM. Each hotline must contend with different technology infrastructures and conflicting international laws. Hotlines encounter different levels of industry, law enforcement and stakeholder awareness and engagement in the issue and have limited resources to support outreach efforts and meet the shifting technology trends surrounding the problem of online CSAM.

Organizations such as INHOPE help amplify the voices of individual hotlines into a community level call to action to improve global awareness of, and response to, the proliferation of CSAM online. This type of global collaboration is necessary and should be expanded in order to have the greatest impact in combating this issue.

While improved technology will lessen the burden of many of the shared challenges facing hotlines, it must be delivered with consideration of limited resources. As such, it is recommended that a technology working group be established to examine current and future technology issues and develop solutions to be shared through the community. The Technology Working Group can bring together the expertise of multiple stakeholders to deliver customizable tools appropriate to current trends and priorities within the hotline community. A community-focused approach can capitalize on shared knowledge and optimize available resources to support and expand hotline capabilities.

The findings presented in this report highlight many areas which can benefit from immediate technical improvements through such a working group. Increased automation can support improved accuracy, free up resources and increase opportunity for content analysis and

victim identification. Expanded data analytics can develop key information and could have sizeable local and global implications in raising awareness of CSAM, facilitating community engagement, and creating new policies concerning the online sexual exploitation of children.

Online sexual abuse and exploitation of children is a global epidemic which can only be fought through collaboration, innovation and determination. Technology plays a vital role in this battle; however efforts must stay relevant to both the issue and the needs of the organizations responding. Hotlines should continue to develop their understanding of online CSAM and ensure those combating it have the technological means to protect children from future victimization.



## Appendix: Hotline Profiles

To ensure a clear picture of the global landscape of hotlines combating online CSAM, a brief profile introducing each hotline was drafted for inclusion in this report. Hotlines were invited to review and contribute to their respective profile prior to the publishing of this report.

<i>ACMA Hotline</i> .....	48	<i>Internet Hotline Cambodia</i> .....	54
<i>Alianza por la Seguridad Internet</i> .....	91	<i>Internet Hotline Center Japan</i> .....	84
<i>Barnaheill—Save the Children Iceland</i> .....	75	<i>Internet Watch Foundation</i> .....	112
<i>Bee Secure Stopline</i> .....	89	<i>jugendschutz.net</i> .....	70
<i>Biztonsagosinternet</i> .....	73	<i>Linea Ciudadano</i> .....	92
<i>Bulgarian Safer Internet Hotline-ARC Fund</i> .....	53	<i>Linha Alerta</i> .....	98
<i>Child Focus</i> .....	51	<i>Meldpunt Kinderporno</i> .....	93
<i>Child Web Alert</i> .....	90	<i>Net Patrola</i> .....	102
<i>CNZD Hotline</i> .....	60	<i>Nettivist</i> .....	66
<i>Cybertip.ca</i> .....	56	<i>Point de Contact</i> .....	67
<i>CyberTipline</i> .....	113	<i>Red Barnet: Save the Children Denmark</i> .....	64
<i>Drossinternets.lv</i> .....	87	<i>Safeline</i> .....	72
<i>Dyzurnet.pl</i> .....	97	<i>SafenetCY</i> .....	61
<i>eco-Beschwerdestelle</i> .....	68	<i>Safer Internet Centre-Russia</i> .....	101
<i>ECPAT Hotline</i> .....	108	<i>Safer Internet LT</i> .....	88
<i>Film and Publication Board Internet Hotline</i> .....	105	<i>Safernet.ro</i> .....	99
<i>Friendly Runet Foundation</i> .....	100	<i>Save the Children Italy</i> .....	81
<i>FSM - Beschwerdestelle</i> .....	69	<i>Seguros en Internet</i> .....	96
<i>Horka Linka</i> .....	63	<i>Spletno Oko</i> .....	104
<i>hotline.ie</i> .....	79	<i>Stopline</i> .....	50
<i>Ihbar Web</i> .....	111	<i>Stopline.sk</i> .....	103
<i>Illegal and Harmful Information Report Center</i> ..	106	<i>Telefono Azzurro</i> .....	82
<i>INHOPE</i> .....	76	<i>Te Protejo</i> .....	58
<i>INHOPE Foundation</i> .....	77	<i>ThaiHotline</i> .....	109
<i>International Forum of Solidarity- Emmaus</i> .....	52	<i>The Orb</i> .....	95
<i>Internet Association of Kazakhstan</i> .....	86	<i>Vihjeliin</i> .....	65
<i>Internet Hotline</i> .....	74	<i>Web547</i> .....	108



## ACMA HOTLINE

Australia

[www.acma.gov.au](http://www.acma.gov.au)

[online@acma.gov.au](mailto:online@acma.gov.au)

The Australian Communications and Media Authority (ACMA) is an independent statutory body of the Australian government with oversight of broadcasting, the Internet, radio and telecommunications. In pursuit of its mission, the ACMA works closely with law enforcement, the media and communications industries, communities, and policy makers. In addition to content regulation and hotline services, the ACMA also offers Internet safety training programs including community outreach, and contributes to issue focused research and regulatory policy development.

The ACMA Hotline became operational in 2000 and serves as the primary reporting mechanism in Australia for potentially illegal or harmful material online, including child sexual abuse material. In addition to child sexual abuse material, reports are made to the hotline regarding terrorism, adult pornography, and material that promotes or instructs in crime or violence.

Reports are made to the Hotline via an online reporting form, as well as by email and fax. Upon receipt of a report, the Hotline assesses the content against classification criteria established under the National Classification Scheme, and undertakes trace analysis to determine where the material is hosted. If the website appears to be hosted by an Australian company, the Hotline partners with Australian law enforcement and the communications industry for an investigation and swift removal of the prohibited content. If hosted internationally, the ACMA refers the content to the relevant law enforcement partner, either through the INHOPE network, or to Interpol (via the Australian Federal Police).

As evidence of the ACMA's close international working relationships, in August 2014, the ACMA Hotline, in conjunction with the Australian Federal Police, hosted the inaugural Combating Child Exploitation Material Online forum, bringing together government, industry and law enforcement partners in the Asia-Pacific region committed to combating online child sexual abuse material.

The forum enabled attendees to exchange strategic and operational information through a range of presentations from public, private, law enforcement and industry bodies. The sessions facilitated discussion of operational tactics and opportunities for innovative collaboration and information-sharing. The forum supported the activities of INHOPE hotlines by providing a regional focus to the global fight against child exploitation online. New and emerging hotlines for reporting child sexual abuse material in Thailand, Cambodia and the Philippines attended the forum.

*(continued from previous page)*

Since its inception in 2000 the hotline has received 33,027 complaints, resulting in 51,574 investigations. In 2014 4,036 complaints regarding potentially harmful material were received, resulting in 8,408 investigations in CSAM.

The ACMA is an active member of the INHOPE global network of hotlines.

In July 2015, the ACMA Hotline will transition into the newly established Office of the Children's e-Safety Commissioner. The Children's e-Safety Commissioner has been established to investigate and remove cyber-bullying material targeted at Australian children from social media platforms and provide a national leadership role in online safety matters. Alastair MacGibbon, founder of the Australian Federal Police's High Tech Crimes Centre, has been appointed to the role of Children's e-Safety Commissioner. The function of the Hotline will remain the same.



STOPLINE  
Austria  
[www.stopleveline.at](http://www.stopleveline.at)  
[office@stopleveline.at](mailto:office@stopleveline.at)

Stopleveline is a non-profit organization and a program of the Austrian Association of Internet Service Providers. It is the online contact point for people who come across child pornography or National Socialist content on the internet in Austria. The mission of the organization is to act as a contact point for people that come across illegal material on the internet with the goal of removing such illegal content, especially online publications in Austria.

Stopleveline actively partners with law enforcement, the internet industry, government/policy makers and social service organizations to remove child pornography, racism/hate speech and national socialist offenses. In addition to accepting reports, the hotline offers other services, including community outreach and internet safety awareness.

Reports are made to the hotline by members of the public via the online reporting form and by email. The Hotline also receives reports from INHOPE member countries. Once the hotline receives the reports, the material is assessed by the hotline analysts and a geographical hosting location is determined. If hosted by an Austrian company, the hotline works with law enforcement and the hosting company to get the content removed from the internet. If hosted internationally, the hotline will refer the report via INHOPE to the appropriate country.

In 2014, the hotline received 8,792 reports, of which 5,895 were in relation to child sexual abuse material. Furthermore, since the hotline became operational in 1998, has received 48,877 total reports. Of these, approximately 34,000 were regarding child sexual abuse material.

## CHILD FOCUS

Belgium

[www.stopchildporno.be](http://www.stopchildporno.be)

[info\\_scp@childfocus.org](mailto:info_scp@childfocus.org)

+32 2 475 44 38



The civil hotline and member of INHOPE, [www.stopchildporno.be](http://www.stopchildporno.be), is a non-profit organization operated and managed by Child Focus, the Foundation for Missing and Sexually Exploited Children. In addition to assisting law enforcement, the hotline aims to inform internet users of the penalization and potential dangers of child pornography online; to instill a sense of responsibility in internet users by raising awareness; and to enable citizens to utilize the hotline.

Established in 2002, the hotline actively partners with law enforcement, the government and policy makers, social service organizations and civilians to combat harmful content on the internet. In addition to possible online child sexual abuse material, the hotline receives missing children reports and sexually exploited children reports. Furthermore, the organization also offers community outreach and internet safety awareness resources, research/policy development, direct victim services and advocate/law enforcement training.

The hotline receives reports via their online reporting form, email and telephone. When reports are made to the hotline, it is directly transferred to the specialized Federal Police departments, based on agreements between Child Focus and the Belgian Law Enforcement Agencies. Child Focus does not qualify the content that is being reported through their civil hotline as illegal or not before sending it to police, as they are not yet able to do so.

In 2014, [www.stopchildporno.be](http://www.stopchildporno.be) received and forwarded 1,432 reports to law enforcement; a number that reaches 26,955 between its launch in 2002 and the end of 2014.



## INTERNATIONAL FORUM OF SOLIDARITY- EMMAUS

SOS Hotline  
Bosnia & Herzegovina  
[www.sigurnodijete.ba](http://www.sigurnodijete.ba)

A program of the International Forum of Solidarity-Emmaus, SOS Hotline serves as a center in Bosnia & Herzegovina for the reporting for inappropriate content and all forms of child abuse through information and communication technologies. Established in 2010, the non-profit Hotline became a permanent member of INHOPE in 2012 as the result of dedication and sustained efforts by the IFS-EMMAUS.

The Hotline actively partners with law enforcement, the internet industry, government/policy makers, social service organizations, schools/community organizations and civilians to achieve their mission and deliver their services. In addition to the processing reports, the hotline offers other services, including community outreach and internet safety awareness, research/policy development, direct victim services, victim identification and advocate/law enforcement training.

The SOS Hotline receives reports primarily through their online reporting form. Reports at the SOS Hotline are received from the public and referred from INHOPE. After reports are received, they are processed and a geographical location for the content is determined. If the content is hosted domestically, reports are forwarded by the analysts to law enforcement. If hosted internationally, reports are referred to the appropriate hotline via INHOPE.

In 2014, the hotline received 8 reports regarding potential child sexual abuse material. Between when IFS-EMMAUS was established in 2010 and the end of 2014, IFS-EMMAUS received a total of 392 reports, 31 of which were made regarding potential CSAM.

The SOS Hotline plays a vital role in the protection of children from sexual exploitation, as evidenced by the following success story: IFS-EMMAUS received a report from a minor through the Hotline application for reporting illegal content. The minor had shared specific private photos with her boyfriend and, after they broke up, the ex-boyfriend published the photos on the web thereby spreading them further. The report was forwarded to the relevant law enforcement agency in Bosnia and Herzegovina and, following the investigation, the police agency succeeded in removing the photos from the respective web sites four days after the report had been received. After the images were removed, feedback was provided to the individual who made the report, as she left her contact details for that purpose, and she was made aware of the removal of her images.

## BULGARIAN SAFER INTERNET HOTLINE-ARC FUND

Bulgaria  
www.web112.net  
+359 2 973 3000



The Bulgarian Safer Internet Hotline is operated by a non-profit organization, the Safer Internet Program of the European Commission. In 2006, the hotline became operational as well as a member of INHOPE. The Hotline was established to act as a mechanism for reporting illegal and harmful content and conduct online, primarily regarding child sexual abuse images or violence against children.

The Hotline actively partners with law enforcement, the internet industry, government/policy makers, schools/community organizations, social service organizations and civilians to accomplish their mission and deliver their services. In addition to receiving reports, the Hotline also offers other services related to community outreach and internet safety awareness, research/policy development and advocate/law enforcement training.

The Hotline receives reports from the public and those referred from INHOPE. In addition to reports regarding child sexual abuse imagery, the hotline also receives reports on a variety of topics, including racism and/or hate speech, drugs, adult pornography, pro-anorexia, suicide, bullying and extreme violence/threats of violence.

Reports can be made to the Hotline via their online reporting form, email and telephone. When reports are made to the hotline, analysts review the reported material to determine if it is illegal or harmful to minors and attempt to identify the geographic hosting location for the material. The analysts will then take the appropriate actions with the report, which may include notifying the relevant hosting company or organization, forwarding to relevant law enforcement and forwarding reports and related information to INHOPE.

In 2014, the Hotline received just over 2,166 reports, of which 117 were regarding child sexual abuse imagery and 33 were confirmed as such. Since its launch in 2006, the hotline was received over 7,700 reports, of which 1,343 were regarding child sexual abuse imagery and 268 were confirmed as such.



# APPLE

## INTERNET HOTLINE CAMBODIA

Cambodia  
www.aplecambodia.org  
info@aplecambodia.org

A program of APLE Cambodia, Internet Hotline Cambodia is an anonymous and confidential forum for reports of child sexual exploitation. APLE Cambodia is a non-governmental organization focused on combating the sexual abuse and exploitation of children through a four prong approach:

- Awareness & Training
- Social Support
- Investigations
- Legal Support

APPLE Cambodia recognizes the importance of partnerships in combating child abuse and works closely with local government, national and foreign law enforcement, the Internet industry, and civil society organizations in pursuit of its mission. In addition to hotline services, APLE offers community outreach and Internet safety awareness initiatives, direct victim services, and training for child protection professionals and national police.

APPLE Cambodia has been operating the child protection hotline since 2010 and receives reports from law enforcement, informants, the public, and other non-governmental organizations. Reports can be made to the hotline via email and telephone. Recently established in 2015, the Internet Hotline currently receives reports on child sexual exploitation activities and materials online. Though still developing its process for report analysis, it will include content assessment, tracing of host country for illegal material, and collaboration with law enforcement for investigation into prohibited content and evidence of local child sexual exploitation.

APPLE is actively engaged with INHOPE to facilitate development of its hotline services and pursue future membership with the global network of hotlines.

APPLE has generously shared the following story as an example of the work being performed by the hotline:

In 2007, APLE started an investigation into a French national called M.C. after he was reported to offer the underage girls one or two dollar for posing in pornographic pictures for him. The case was immediately reported to police by APLE; however, none of the possible victims disclosed abuse when interviewed at the station because they were afraid of losing the relationship of support M.C. had established with them.

*(continued next page)*

*(continued from previous page)*

APPLE continued to investigate the case in depth and found more evidence leading to the arrest of M.C. and his girlfriend in 2011. At the station, he confessed to producing child pornography and selling them online. Eight girls testified at the station that they had been exploited by M.C.

The case is not unusual for APPLE. In more than ten percent of all investigations into child sexual abuse and exploitation that led to an arrest, child pornography plays a role. In slightly more than 15 percent of these cases, the offenders only possess child pornography, while in less than 85 percent of the cases, the offenders actually produced child pornography.

In the case of M.C., all victims were provided with social as well as legal support from APPLE. The youngest victim was only 6 years old at the time of the abuse. With the help of proper counseling and support, she is now continuing her study. At the time of the abuse, she did not know that she was being used for pornographic purposes; she thought it was normal to take such photos. Thanks to APPLE's social worker, she learned about her rights as a child and how she can protect herself in the future.

M.C. and his girlfriend had to stand trial and were convicted for producing child pornography. They were sentenced to 5 years each. M.C. was also ordered to be deported after his imprisonment. In addition, he had to pay 1250 dollar to each of his victims.

As a result of being confronted with child pornography cases, APPLE has launched an Online Hotline in the beginning of 2015. The hotline aims to collect, disseminate and investigate reports from the general public, law enforcement, other NGOs, regarding suspected cases of online child exploitation. Through this hotline, APPLE aims to better protect children against online exploitation in Cambodia and worldwide.



CYBERTIP.CA  
Canada  
www.cybertip.ca  
1-204-945-5735

Cybertip.ca is a non-profit organization established as a program of the Canadian Centre for Child Protection that serves as the national tipline for reporting the online sexual exploitation of children. The Canadian Centre for Child Protection is a charitable organization dedicated to the personal safety of all children. Specifically, they aim to reduce child victimization by providing national programs and services to the Canadian public.

Cybertip.ca has been in operation since 2002, and became a member of INHOPE in 2005. The hotline works closely with law enforcement, the internet industry, government/policy makers, social service organizations and schools/community groups to accomplish their mission and deliver their services to Canadians. In addition to receiving reports, the hotline also offers additional services related to community outreach/internet safety awareness, research/policy development and direct victim support services.

The Hotline receives reports via their online reporting form, email and telephone. Reports regarding child sexual abuse material come from a variety of sources, including the public, law enforcement, the internet industry and other INHOPE hotlines. In addition to reports regarding child sexual abuse material, Cybertip.ca also receives and processes reports regarding online luring, child exploitation through prostitution, travelling to sexually exploit children, child trafficking, making sexually explicit material available to children, agreements or arrangements with another person to commit a sexual offense against a child and the non-consensual distribution of intimate images involving individuals under the age of 18.

When Cybertip.ca receives a report pertaining to child sexual abuse material, the content is viewed and assessed and, when possible, a geographical hosting location is determined. When content is hosted in Canada, relevant agencies are contacted, including law enforcement and hosting providers. When content is hosted internationally, it is referred via the INHOPE global network of hotlines to an organization in the country of the content.

In 2014, the hotline received a total of 33,082 reports, 31,994 of which were regarding potential CSAM. Overall, the hotline has received 135,155 total reports between the time of its inception and the end of 2014, 127,855 of which were regarding CSAM.

Cybertip.ca plays a vital role in the protection of children from sexual exploitation, as evidenced by the following success story:

In 2013, the Toronto Police Service (with representation from the Canadian Centre for Child Protection) announced the results of Project SPADE, an investigation stemming in part from reports made to Cybertip.ca.

*(continued next page)*

*(continued from previous page)*

These reports helped law enforcement to identify websites that, upon further investigation, have led to the removal of nearly 400 children from abusive environments and to the arrest of close to 350 offenders from around the world, many of whom were involved in professions or volunteer work that provided close contact with children.

This highlights the importance of child-serving organizations having the tools in place to help reduce the likelihood that an offender will successfully gain access to and sexually abuse a child in their care. One such tool is the Canadian Centre for Child Protection's Commit to Kids program (<http://committokids.ca>). Specifically tailored to assist child-serving organizations in creating safer environments for the children in their care, this program provides organizations with a step-by-step plan using a risk-management approach that goes far beyond criminal record checks to prevent child sexual abuse.



TE PROTEJO  
Colombia  
www.teprotejo.org

A program of Colombia's Red PaPaz, Te Protejo was established as a mechanism for reports to be made regarding child sexual abuse material and sexual exploitation. Red PaPaz is a non-profit organization and civilian force that attempts to encourage the positive cultural environment for children and adolescents by influencing citizens, the state media communication and other organizations to comply with relevant laws and be socially responsible.

Established in 2012, Te Protejo became the first INHOPE Foundation member. They work closely with law enforcement, the internet industry, schools/community groups, government/policy makers, social service organizations and civilians to deliver their services. In addition to online child sexual abuse material, Te Protejo receives and processes a variety of other report types, including commercial sexual exploitation of children, school bullying, cyber-bullying, inappropriate content in media, sale of alcohol and other substances to children under 18 years old, child abuse, labor or neglect, and any other situations that may affect children under 18 years old.

Reports are made primarily via the online reporting form but also by smartphone app by members of the public as well as INHOPE member countries. Once the content has been reviewed, domestic reports are forwarded to relevant enforcement and international reports are referred to the appropriate INHOPE member country.

In 2014, Te Protejo received 6,452, of which 3,724 reports were regarding potential CSAM. Furthermore, the hotline received 12,565 total reports between its inception in 2012 and the end of 2014, of which 5,683 were regarding potential CSAM.

The SOS Hotline plays a vital role in the protection of children from sexual exploitation, as evidenced by the following two hotline highlights:

When Te Protejo became operational, the process of blocking CSAM took approximately two to four months, so Te Protejo started to pressure the ISP and government (Ministry of Information Technology and Communications) to reduce the time of the process.

*(continued next page)*

*(continued from previous page)*

On 2013, Red PaPaz started a petition which was signed by over 40,000 people, asking the ISP to comply with Colombian law that requires them to block CSAM (only illegal material on web) and demanding that the TIC

Ministry punish noncompliance. As a result of this petition, the Ministry of Information Technology and Communications and many ISP signed an MOU “Cero Tolerance with child sexual abuse material” committing to fight against CSAM as well as strength routes allegations of this crime in Colombia, by reporting this content in Te Protejo.

On July 2014, Te Protejo held the II International Meeting for the management and prevention of child sexual exploitation online, Conectados para protegerte. At this meeting, the MOU was ratified by delegates from various offices and organizations, including the Min ICT and Min CIT, Ministry of Labour, Ministry of Education, ICBF, Contraloria General de la Nación, the Attorney General’s Office, National Police, Dijin Cybercrime, Microsoft, McAfee, ETB, Telefónica, Google, ICMEC, INHOPE, CCIT, Internet and telephony operators and others.



## CNZD HOTLINE

Croatia  
[www.cnzd.org](http://www.cnzd.org)

Established in 2006, the Center for Missing & Exploited Children (Croatia) (CNZD) began operating a hotline for reporting material online that depicts or encourages the sexual exploitation of children in 2012. The CNZD was created to fill a void in state services to protect children online and works closely with law enforcement, families, community organizations, and policy makers in pursuit of this mission. In addition to hotline services, CNZD is a member of Missing Children Europe and works closely with children with behavioral problems. CNZD also delivers Internet safety awareness programs, contributes to research and policy development, and offers direct victim services.

Reports are made by the public to the hotline via online reporting form. In addition to reports regarding possible child sexual abuse material, the hotline receives complaints concerning racism/hate speech, gambling, substance abuse, self-harm, and bullying. Upon receipt of a report, a hotline analyst will review the content and attempt to determine the country hosting the prohibited content. If residing in Croatia, the hotline partners with law enforcement and the internet industry for further investigation into the report and swift removal of the content. If hosted internationally, CNZD forwards the report via the INHOPE network to a hotline in the country hosting the website.

Since its launch, the hotline has received 287 reports and in 2014 received 84 reports.

CNZD is a member of the INHOPE network of hotlines.

## SAFENETCY

Cyprus

[www.cyberethics.info](http://www.cyberethics.info)

[reports@cyberethics.info](mailto:reports@cyberethics.info)

+35722873820



A component of the CyberEthics project, the SafenetCY hotline was established to help promote safe use of the internet in Cyprus by acting as a mechanism for the reporting of illegal and harmful material and activities online. CyberEthics was established as a non-profit project by the Safer Internet plus Program of the European Commission and includes the SafenetCY hotline as well as the Awareness Node and Helpline. The hotline became a member of INHOPE in 2008.

SafenetCY receives reports about a variety of issues related to online child sexual abuse material, including child pornography, child erotica, child nudism, child grooming activities, child trafficking and child sex tourism. In addition, the hotline also receives and processes reports about racism and gender discrimination.

SafenetCY actively works with law enforcement, the internet industry, schools/community groups, government/policy makers, social service organizations and civilians to achieve their mission and deliver their services. In addition to receiving reports, the hotline offers additional services related to community outreach/internet safety awareness and research/policy development.

Reports are made to the hotline via their online reporting form, email, telephone and smartphone app by members of the public as well as INHOPE. The material is assessed by hotline analysts and a geographical host location is determined. If it is hosted domestically, analysts will forward the report to law enforcement and may refer the report to their organization's helpline if it requires child welfare attention. If hosted internationally, the analysts will forward the report to the relevant country or to INHOPE to the appropriate country's hotline.

In 2014, SafenetCY received 238 reports, and has received 1358 total reports since their inception in 2008.

The SafenetCY hotline plays a vital role in the protection of children from sexual exploitation, as evidenced by the following success story:

In December 2013, the Cyprus Hotline received a report from a 14 year old boy, who reported a possibly fake Facebook profile of someone claiming to be a girl. As the boy told us, this person also approached some of his friends, and after chatting with them for a while, deceived the children into providing naked pictures of themselves. The boy did not wish to report the incident to the Police

*(continued from previous page)*

and contacted us for help. Upon receiving the complaint, the hotline forwarded the case to the Police while preserving the anonymity of the boy.

The Cyber Crime Unit of the Cyprus Police, after thorough investigation of the report, managed to locate the person behind the fake Facebook profile. The person was an 18 year old soldier. At his house, the police found 128 pictures of naked boys and 13 videos of CSAM depicting boys and girls aged 10 to 14 years old. Additionally, in one of those videos, a young boy is depicted to engage in sexual contact with an older teenager (or young adult), who is possibly the 18 year old offender.

In the investigation the offender admitted the creation of a fake Facebook profile as well as his quest to find young boys through it. According to the Police, around 30 boys have sent him naked pictures. To date, this case was one of the most serious cases that the Cyber Crime Unit dealt with at the time, and the court ordered his arrest. The case and the offender are currently awaiting trial with the outcome to be determined. However, this is a good example for the Cypriot society that reporting can help as we can act on their behalf to the Police and convict offenders.

## HORKA LINKA

Czech Republic  
[www.horkalinkaczi.cz](http://www.horkalinkaczi.cz)



## Horká linka

Established in 2009, Horka Linka functions as a reporting mechanism for the public regarding potentially illegal online content. Horka Linka is the only independent hotline operating in the Czech Republic. Reports are made to the hotline by members of the public via email or web based reporting form. Horka Linka receives reports regarding potentially illegal material including, but not limited to, child sexual abuse material, child sex trafficking, bullying, self-harm, and racism.

Upon receipt of a complaint, hotline analysts review reported content to determine if it is illegal according to local laws and if it is hosted in the Czech Republic. Based on the analysis conducted, reports may be forwarded directly to Czech law enforcement or referred to a fellow member of the INHOPE network. In support of their mission, the hotline actively collaborates with Czech law enforcement, electronic service providers, and area policy makers.

Since its inception, Horka Linka has received over 15,000 reports regarding prohibited material. In 2014, the hotline received 3986 unique reports, 562 of them was evaluated as child sexual abuse material.

Horka Linka is part of the larger Czech Safer Internet Centre and an active member of INHOPE.



RED BARNET: SAVE THE  
CHILDREN DENMARK  
Denmark  
[www.savethechildren.dk](http://www.savethechildren.dk)

A program of the international non-profit organization, Save the Children, Save the Children Denmark was established to work with local communities to put children's rights on the public and political agenda. The focus of the organization is to inspire breakthroughs in the way the world treats children, and to achieve immediate and lasting change in their lives. To help achieve this goal, the hotline functions as a mechanism for reports to be made regarding online child sexual abuse material.

While the hotline became operational in 1998, it was established as the Danish hotline for the Save the Children organization in 2001. Save the Children Denmark actively works with law enforcement, the internet industry, government and policy makers, schools and civilians to deliver their services. In addition to the hotline, Save the Children Denmark also offers other services related to community outreach and internet safety awareness, research/policy development, direct victim services and advocate/law enforcement training.

Reports are made to the hotline via their online reporting form, email and telephone by members of the public as well as INHOPE and then processed by hotline analysts. Analysts initially trace the origin of the content and assess it to determine if it is illegal material. If the report content refers to a domestic location, or a country in which no hotline exists, notification will be sent to the Danish national police. In contrast, if the material is hosted in another country that has a hotline, the appropriate hotline will be informed via INHOPE.

In 2014, Save the Children Denmark received 2,568 reports, of which, 799 reports with potentially illegal content was forwarded. Between 2001 and the end of 2014, the hotline has received over 71,000 total reports, of which approximately 20,000 were forwarded as potentially illegal reports.

The SOS Hotline plays a vital role in the protection of children from sexual exploitation, as evidenced by the following hotline highlights:

The organization co-operates with "Break the Circle", a program aimed at adults with a sexual interest in children (operated by the Clinic of Sexology at the State Hospital). In addition, in 2014 and 2015, Save the Children trained more than 250 professionals (police officers, doctors, psychologists, social workers) to tackle the implications of the use of online media in sexual abuse of children.

**VIHJELIIN**

Estonia

www.vihjeliin.ee

vihje@vihjeliin.ee

+372 6311 128

Teavita  
illegaalsest sisust  
**Vihjeliinile**



Estonia's Vihjeliin hotline was established by the Estonian Union for Child Welfare as a service to prevent the distribution of materials that violate the rights, dignity and physical inviolability of children on the internet. The hotline and its larger organization work closely with other national organizations, including law enforcement authorities, the internet industry and other non-profit organizations such as INSAFE and INHOPE. The hotline became both operational and a member of INHOPE in 2011 and functions as a mechanism for reporting material online depicting illegal content, particularly presenting the sexual abuse or exploitation of minors and child trafficking.

Vihjeliin works closely with law enforcement, the internet industry, government/policy makers, social service organizations, schools/community groups and civilians to achieve its mission and deliver its services. In addition to responding to reports, the hotline also offers additional services related to community outreach and internet safety awareness, research/policy development and advocate/law enforcement training.

Reports are made to the hotline via their online reporting form and through email by members of the public, law enforcement and INHOPE. When reports are made to the hotline, analysts assess the content and attempt to trace the geographical hosting location of the content. Based on where the host is located, the analysts will forward the report to law enforcement authorities and INHOPE to the appropriate member country's hotline.

From the time of its establishment in 2011 to March 2015, Vihjeliin has received 3,333 reports--335 of which contained information about CSAM. In 2014 alone, the hotline received 1,040 reports, 127 of which were regarding CSAM.

Vihjeliin plays a vital role in the protection of children from sexual exploitation, as evidenced in this hotline highlight:

Vihjeliin has had successful cooperation with their Finnish colleagues, who produced the book, "Protect me from everything: Information for specialists working with children about how internet and digital devices are being used for the sexual abuse of children". The Estonian Hotline team translated and adapted the book in cooperation with Estonian specialists. Since then, they have introduced and disseminated the book via different events (seminars, online, etc.) and, according to feedback from specialists, the book has proven very useful for them in their daily work.



## NETTIVIHJE

Finland

[www.pelastakaalapset-fi](http://www.pelastakaalapset-fi)

[netti@pelastakaalapset.fi](mailto:netti@pelastakaalapset.fi)

A program of Save the Children, Finland, Nettivist serves as a mechanism for the public to report apparent child sexual abuse material circulating the Internet. Save the Children, Finland is part of Save the Children International. Since 1922, the organization has been fighting for the rights of children in Finland and around the world through activities including direct child protection, international programs, and community outreach and advocacy. Save the Children, Finland is part of Finland's Safer Internet Centre and is a member of INHOPE.

Nettivist has been operational since 2002. The hotline works to promote detection and deletion of illegal child sexual abuse material on the Internet, and to identify children that are subjected to sexual abuse through national and international co-operation. In addition to reports of online child sexual abuse material, the hotline receives reports regarding racism and xenophobia and extreme adult content.

Nettivist works closely with law enforcement to remove child sexual abuse material from the Internet. Upon receipt of a report regarding potentially illegal material, a hotline analyst will review the material and, if illegal, will attempt to locate where the material is hosted. If a company in Finland, reports are directly forwarded to local law enforcement for further investigation and removal of the content. If hosted internationally, the report is forwarded to an INHOPE member hotline in the area hosting the website. Information of all illegal material hosted anywhere in the world is also forwarded to law enforcement.

In 2014, Nettivist received 2,307 reports regarding possible child sexual abuse material. Of these reports, 18 % (409) were assessed to refer to illegal content based on the national legislation.

Between 2003 and 2014 Nettivist has processed 55,373 reports referring to potentially illegal material, of which 39 % (21,531) have been assessed as illegal. The proportion of illegal content has been descendent.

Nettivist has been a partner in the BIK NET (Better Internet for Kids Network Pilot) project, and piloted a new technical solution IC-CAM (I see Child Abuse material) to enhance the processing of potentially illegal material. In March 2015, Nettivist processed nearly 13,000 images and videos through IC CAM which referred to potentially illegal material.

## POINT DE CONTACT

France

[www.pointdecontact.net](http://www.pointdecontact.net)

[contact@pointdecontact.net](mailto:contact@pointdecontact.net)



A program of the French Internet Service Providers Association (AFA), the Point de Contact hotline was initially established as a public mechanism for reporting potential child sexual abuse material and online hate speech.

Established in 1998, Point de Contact was born out of the desire by AFA to contribute to the fight against harmful content on the Internet. Point de Contact actively partners with the Internet industry, law enforcement and the government to deliver their services. In addition to online child sexual abuse material, the hotline receives reports including but not limited to Incitement to Violence, Incitement to Suicide and Incitement to Terrorism.

Reports are made to the hotline by members of the public and then assessed by content analysts, which review the reported material to determine if it is illegal under French law and attempt to identify its geographic hosting location. If hosted by a French company, local law enforcement will be alerted and the hosting provider will be notified to remove the content. If hosted internationally and assessed as child sexual abuse material, the report is forwarded via INHOPE to the appropriate member country's hotline.

In 2014, Point de Contact received almost 6,000 reports regarding potentially illegal content on the Internet, and since its launch in 1998 has received over 100,000 reports.

In addition to hotline services, Point de Contact is also involved in awareness raising actions targeting young Internet users, and has recently started a series of short educational comics, which are distributed for free to schools, social workers, etc. The first two respectively deal with the issues of grooming and sexting and have been a big success.

Point de Contact is part of the French Safer Internet Centre and is a founding member of INHOPE.



ECO-BESCHWERDESTELLE  
Germany  
[www.eco.de/services/internet-beschwerdestelle](http://www.eco.de/services/internet-beschwerdestelle)  
hotline@eco.de

eco – Beschwerdestelle is a program of eco, the Association of the German Internet Industry. The parent organization, eco, was founded in 1995. Made up of around 800 members in the Internet industry, eco represents the interests of its membership both nationally and internationally.

eco added the hotline service in 1996 to combat potentially illegal and harmful content on the Internet. It has a self-regulatory approach. In addition to reports of possible child sexual abuse material, the hotline receives reports on areas including but not limited to SPAM, Racism & Xenophobia, hate speech, adult pornography, and self-harm.

Upon receipt of a complaint, eco analysts review the content and attempt to identify where the material is located if it is deemed actionable. If hosted on German servers, eco collaborates with (local) law enforcement and the appropriate Internet Service Provider for prompt removal of the material and investigation into its poster. Since 2010 eco has been gathering statistics on the Notice & Takedown of CSAM. The statistics continuously show swift removal of CSAM after notifying the host service provider or INHOPE partner hotline. In regard to content hosted in Germany, in 2014 URLs were removed on average 2.94 days after the site was reported to the eco hotline (incl. weekends and public holidays).

If hosted abroad in a country with an INHOPE partner hotline, the report is forwarded via the INHOPE network to the hotline in the country in which the content is located. If no INHOPE member hotline exists, or if the report is outside the hotline's scope of action, eco notifies the host service provider for prompt removal of the material. In regard to CSAM, the eco hotline is obliged to report all cases to the German Federal Criminal Police (BKA), regardless of whether the content is hosted in Germany or not.

The hotline collaborates closely with law enforcement, policy makers, and Internet Service Providers to remove potentially harmful material from the Internet. In 2014, the hotline received over 135,000 reports, the majority of which were identified as possible child exploitation material.

eco is part of the German Safer Internet Centre and is a founding member of INHOPE.

## FSM - BESCHWERDESTELLE

Germany  
www.fsm.de  
hotline@fsm.de



FSM, or Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, provides hotline services through FSM – Beschwerdestelle. FSM is a self-regulatory non-profit membership organization for the Internet and Communications industry. FSM focuses on the protection of young people on the Internet and advising their members in all questions regarding youth protection matters and in addition to offering hotline services FSM establishes criteria for content standards and offers online safety education for children and the community.

The FSM Hotline deals with all content which is illegal or harmful to minors under The Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia (JMStV). In 2014, the hotline received 4,949 complaints of potentially illegal material, 1,067 of which were proven to be CSAM.

Reports are received to the hotline via email, fax, web report, or smartphone app. Upon receipt, analysts assess the nature of the reported material and attempt to identify a jurisdiction for the illegal material. If the material is hosted by a German company or if the site owner resides in Germany, FSM works closely with law enforcement and Internet Service Providers to support investigative efforts and ensure prompt removal of the illegal material. If resting outside of Germany, CSAM reports are forwarded to the appropriate member hotline via INHOPE and via German LEA. German hotlines are a vital partner to bridge the gap between law enforcement and the public. In 2014, the hotlines referrals were responsible for 92% of the CSAM URLs investigated by German law enforcement.

FSM is a member of the German Safer Internet Centre and is a founding member of INHOPE.



JUGENDSCHUTZ.NET

Germany

www.jugendschutz.net

hotline@jugendschutz.net

The German hotline jugendschutz.net was launched in 1997. jugendschutz.net is a non-profit organization which, in addition to hotline services, provides oversight of the German media services, offers community outreach and Internet safety training, and participates in research and policy development.

The hotline acts as a reporting mechanism for content that may be illegal, harmful to children, or pose potential to impair a child's development. In pursuit of its mission, jugendschutz.net works closely with law enforcement, internet service providers, youth protection organizations, and policy makers. Reports may be made to the hotline via email, fax, telephone, or online reporting form. In addition to apparent child sexual abuse material, the hotline receives reports concerning racism/hate speech, adult pornography, pro-anorexia and self-harm material, bullying, and drugs.

Upon receipt of a report, a member of the hotline staff reviews the content and attempts to identify the country in which the material is hosted. If hosted by a German company, jugendschutz.net will collaborate with local law enforcement for investigation and removal of the material. If the material originates outside of Germany, a report is forwarded to the appropriate hotline via the INHOPE network.

Since its launch in 1997, jugendschutz.net has received around 85,000 reports and processed more than 150,000 URLs of potentially illegal and harmful material.

jugendschutz.net is a part of the German Safer Internet Centre and was a founding member of INHOPE.

jugendschutz.net has generously provided the following to introduce its hotline:

jugendschutz.net aims at developing an overall strategy for combating CSAM, not only child pornography, but also depictions in the 'grey area'. These are not illegal in most countries, but according to the German legislation this content falls under the definition of child sexual exploitation and it is illegal since 2003; most of the content is hosted abroad.

*(continued next page)*

*(continued from previous page)*

jugendschutz.net has conducted intensive research in this area for several years (e.g. model sites, boy/girl lover forums). During the latest research in 2014, jugendschutz.net checked 280 internet destinations - websites and social web content. jugendschutz.net contacted providers, informed them about the content, referred to their Terms of Service and achieved removal of 78 % of the content.

Since November 2014, a competence center 'No Grey Areas' was established within jugendschutz.net. Here, jugendschutz.net will systematically gather knowledge about content in the 'grey area' and develop strategic countermeasures, remove the platforms for this content and support internet industry in terms of proactive measures.

In the network 'No Grey Areas' coordinated by the German Center for Child Protection on the Internet (I-KiZ) jugendschutz.net joins efforts with other partners (Google, FSM) to combat content in the 'grey area'; international partners shall follow in 2015.



SAFELINE  
Greece  
[www.safeline.gr](http://www.safeline.gr)  
[contact@safeline.gr](mailto:contact@safeline.gr)

A program of the Institute of Computer Science, Foundation for Research & Technology-Hellas, SafeLine is a mechanism for reporting illegal material found on the Internet, with particular focus on child sexual exploitation. The hotline became operational in 2003 and partners closely with law enforcement, families, community organizations, the Internet industry and policy makers in pursuit of its mission. In addition to hotline services, the organization offers outreach and Internet safety awareness programs and contributes to research and policy development in the interest of a safe Internet.

The hotline receives reports via email, smartphone app, and online reporting form. In addition to apparent child sexual abuse imagery, the hotline also receives reports regarding racism/hate speech, bullying, and self-harm material. Upon receipt of a report, the hotline assesses the potentially illegal content and attempts to identify in which country the website is hosted. If a Greek hosting company, the hotline forwards the report to local law enforcement for further investigation and works with the hosting company for quick removal of the illegal material. If hosted internationally, SafeLine seeks a hotline in the hosting country via the INHOPE network of hotlines and the report is forwarded for further action.

In 2014, 3,435 cases were reported to the Safeline hotline; of these, 14 went on for possible prosecution.

SafeLine is part of the Greek Safer Internet Centre and is a member of INHOPE.

## BIZTONSAGOSINTERNET

Hungary

[www.biztonsagosinternet.hu/en](http://www.biztonsagosinternet.hu/en)

[bejelentes@biztonsagosinternet.hu](mailto:bejelentes@biztonsagosinternet.hu)



Biztonsagosinternet, established in 2011, is a program of the Theodore Puskas Foundation. The hotline strives to remove any illegal or potentially harmful material from the Internet, with particular attention given to child sexual abuse material. In addition to reports concerning child abuse imagery, the hotline receives complaints regarding SPAM, racism, adult pornography, bullying, and enticement to drug use.

Reports are primarily submitted via online reporting form however concerns can be emailed as well. Upon receipt of a report, an analyst with the hotline reviews the material in question. If illegal or harmful to children, the hotline will attempt to locate where the website is hosted. In cases where the content is hosted in Hungary, the hotline works closely with hosting services to remove content and law enforcement when applicable to ensure a prompt investigation. When the material is hosted internationally, reports are forwarded via the INHOPE network to a local hotline that can assist.

Biztonsagosinternet is part of the Hungarian Safer Internet Centre and is a member of the global network of hotlines, INHOPE.



## INTERNET HOTLINE

Hungary

<http://english.internethotline.hu>  
[internethotline@internethotline.hu](mailto:internethotline@internethotline.hu)

Hungary's Internet Hotline is an initiative of the Hungarian National Media and Information Communications Authority. The Authority is a government organization tasked with ensuring the undisturbed operation of information and communications technology, with particular attention given to the interests of users.

The Internet Hotline has been operational since 2005. The Hungarian National Media and Infocommunications Authority began hosting the program in 2011. Prior to this time it was operated by the Hungarian Association of Content Industry. The hotline is a reporting mechanism for possibly unlawful or harmful material to minors and works closely with law enforcement, Internet Service Providers, policy makers, and community organizations in pursuit of its mission. In addition to reports concerning possible child sexual abuse material, the hotline receives complaints which include, but are not limited to, racism/hate speech, adult pornography, self-harm, and bullying.

Reports are made to the hotline via online reporting form or email. Upon receipt, an analyst first reviews the reported content to determine if it is illegal or potentially harmful to minors. The analyst will attempt to locate where the website is hosted and if within Hungary will pursue removal of the content with the relevant service provider. If the material is illegal, law enforcement will be notified to begin an investigation. If the material is hosted outside of Hungary, a report will be forwarded via INHOPE to the appropriate hotline.

In 2013 the hotline received almost 500 reports of material which may be illegal or harmful to minors.

The Internet Hotline is an active member in the global network of hotlines, INHOPE.

## BARNAHEILL—SAVE THE CHILDREN ICELAND

Iceland

[www.barnaheill.is](http://www.barnaheill.is)

[Barnaheill@barnaheill.is](mailto:Barnaheill@barnaheill.is)

+354 553 5900



Barnaheill - Save the Children Iceland was established in 1989 and is a part of Save the Children International. The organization advocates on children's rights, promotes participation of children and works on and supports projects both in Iceland and abroad. The focus of the organization is to inspire breakthroughs in the way the world treats children, and to achieve immediate and lasting change in their lives. From the beginning the main focus of Barnaheill – Save the Children Iceland's work is protecting children from all kinds of violence, especially sexual abuse in connection with the internet. Since 2001, Barnaheill - Save the Children Iceland has participated in the international project Stop Child Pornography on the Internet. The EU's Safer Internet Programme has provided support to the project, which has the objective of advocating safety and working against illegal and harmful content on the Net.

At the center of the project is the Hotline, which became operational in 2001 and is a full member of INHOPE. The organization actively partners with law enforcement and government/policy officials to deliver their services. In addition to possible online child sexual abuse material, the hotline also receives reports regarding racism and/or hate speech, adult pornography and bullying. Furthermore, Save the Children Iceland also offers other services related to community outreach and internet safety awareness, research/policy development, and advocate/law enforcement training.

Reports are made to the hotline by members of the public as well as INHOPE hotlines and forwarded to the relevant law enforcement and/or forwarded via INHOPE to the appropriate member country's hotline. In 2014, Save the Children Iceland received 930 reports, of which 98 of them were regarding child sexual abuse material. Furthermore, since its launch in 2001, has received over 4,000 total reports.

The hotline plays a vital role in the protection of children from sexual exploitation, as evidenced by the following hotline highlight:

Icelandic law states that those who sexually offend children abroad can be prosecuted in Iceland, even if it is not a crime in the country of abuse. To educate people about this law and child exploitation, Save the Children Iceland has produced and distributed posters in cooperation with the Icelandic Healthcare for people visiting Iceland or going abroad. For example, posters are displayed at the international airport in Keflavik with urgent messages to travelers about sex tourism, the laws and the importance of reporting.



**INHOPE**  
International  
www.inhope.org  
info@inhope.org  
+31 (0) 20 570 0296

INHOPE is a global network of Internet hotlines made up of two affiliated organizations which work in close collaboration, the International Association of Internet Hotlines (INHOPE) – a membership association established in 1999 by the European Commission and the INHOPE Foundation- a charitable foundation established in the Netherlands in 2010 with the aim of helping develop new hotlines worldwide, particularly in emerging countries where there is a lack of funding or even legislation.

The members of the INHOPE network are served and represented by the INHOPE Secretariat, which has its Headquarters in Amsterdam, the Netherlands.

INHOPE member hotlines are represented by a diverse base and include ISP Associations, Government agencies and Non-governmental organizations.

INHOPE has 51 members in 45 countries across Europe, the Americas, Africa and Asia Pacific all of whom respond to reports of illegal online content from the public. The unifying factor of their membership is that they all receive and respond to reports of child sexual abuse material and have a vision of an Internet free from Child Sexual Abuse Material (CSAM).

INHOPE is the administrator of the INHOPE Report Management System, an international platform for the Exchange of URLs containing CSAM between national hotlines, with the specific aim of channeling reports to the hotline in the hosting country for removal of public access and potential investigation by law enforcement.

INHOPE also coordinates a program known as IC-CAM (started as part of the BIK-NET Project in 2014) which aims to increase and enhance the use of hashing technology in content review. The system has been piloted by 12 hotlines and is currently being further enhanced and rolled out (as part of European Commission's Tender "Digital Service Infrastructure for making a better and safer Internet for Children" LOT 2) in a number of additional European hotlines.

In addition, INHOPE is empowered by its members to do the following:

- Best Practice development
- Quality Assurance of hotlines procedures to ensure the fast removal of CSAM
- Training
- Publication and dissemination of statistics on global hosting of CSAM
- Trend analysis
- Inform and provide evidence to policy makers at the international level

## INHOPE FOUNDATION

International  
www.inhopefoundation.org  
enquiries@inhopefoundation.org



The rapid expansion of the Internet and forms of criminality associated with technological advancements has overcome the capacity of governments and civil society in many countries to respond to the growing problem and new reality of CSAM.

In recognition of the logistical and financial obstacles that many organizations face in establishing an Internet Hotline, INHOPE created the INHOPE Foundation.

Established in 2010, the INHOPE Foundation ([www.inhopefoundation.org](http://www.inhopefoundation.org)) was conceived as a vehicle to raise funds to support the set-up of organizations wishing to establish an Internet Hotline, especially in emerging markets.

In addition, the INHOPE Foundation facilitates training, translation services and consultancy.

Foundation participants will benefit from their affiliation with the INHOPE network. It provides them with global visibility through a variety of communication channels, opportunities to access best practice in all areas of hotline work through workshops and training and the opportunity to build personal relationships with the wider INHOPE membership and ultimately be a part of the global INHOPE network.

Given the importance of a sustainable and autonomous local base for any national Hotline, the INHOPE Foundation is unable to financially support any general, administrative or salary costs for organizations with which it cooperates.

Before being accepted as a Foundation Participant, the candidate organization and the INHOPE Foundation work together to establish the capacity and potential of the organization to operate a Hotline in their country.

Becoming a Foundation Participant of the INHOPE Foundation implies and requires a cooperation of 2-3 years, during which period the Foundation Participant commits to set up or strengthen their national Hotline, work towards establishing a sustainable local base, and to develop protocols that conform to the quality standards required for Membership of INHOPE.

A *Provisional* Participant can become a *Full* Participant once the Hotline is operational and after presentation to the INHOPE Membership for a vote. This provides the Participant with honorary access to the INHOPE Report Management System so that it can begin to submit and

receive reports of URLs containing CSAM within the global network.

After the initial period, it is expected that the Participant will be ready to apply for INHOPE membership and participate in the membership fee structure in exchange for services offered by INHOPE.

**HOTLINE.IE**

Ireland  
 www.hotline.ie  
 report@hotline.ie



The Irish hotline, hotline.ie, is a program of the Internet Service Providers Association of Ireland (ISPAI). ISPAI is a self-regulating organization of 53 member Internet Service Providers. In addition to running the hotline, ISPAI presents a united front for issues concerning Irish Internet Service Providers and has established the Code of Practice and Ethics to which all members must adhere.

Hotline.ie was established in 1999 to serve as a reporting mechanism for suspected illegal content, with special focus on child sexual abuse material. Along with hotline services, hotline.ie also offers community outreach and Internet safety awareness, and advocate, law enforcement, and Internet service provider training. The hotline actively partners with law enforcement, the Internet industry, parents and guardians, and policy makers in pursuit of their mission. In addition to reports concerning possible child sexual abuse material, hotline.ie also receives reports concerning racism/hate speech and financial scam sites.

Reports are made to the hotline via email, telephone, postal service, online reporting form, and smartphone app. Upon receipt of a report, the material is assessed by hotline staff and traced to identify the country in which it is hosted. If originating from within Ireland, hotline.ie collaborates with Irish law enforcement and ISPAI member hotlines to ensure a thorough investigation and rapid removal of the material from the web. If hosted internationally, a report is forwarded to a hotline in the hosting country via the INHOPE network.

At the writing of this report, the hotline has received more than 33,000 reports since its launch in 1999. In 2014, the hotline received almost 5,000 reports, 3,203 of which were regarding suspected CSAM.

Hotline.ie is part of the Irish Safer Internet Centre and is a founding member of INHOPE.

The hotline has generously provided the following case example underscoring the importance of global collaboration:

**REPORTS TO HOTLINE.IE LEAD TO ARRESTS IN CALIFORNIA AND BULGARIA** A report received by the Hotline in 2008 led to an arrest in the US during 2010. The Hotline Content Analyst investigated the report in July 2008, and forwarded the results to the relevant parties for investigation. This resulted in the information being passed to the Los Angeles Police Department.

*(continued from previous page)*

The offender was arrested in August 2010 and pleaded guilty to the charges. He was sentenced in October 2010 to six years in prison and was registered as a sex offender.

In April 2011, an anonymous report was submitted to Hotline.ie detailing a suspiciously named file which was being shared on the Bit Torrent peer-to-peer network. After successfully connecting to the Bit Torrent swarm where the content was being distributed, the Hotline Analyst traced an IP address in Bulgaria from which a video of a scene with two boys engaging in sexual activity with two girls was shared. The estimated age of the boys was 8 to 10 years old, and the estimated age of the girls was 10 to 12 years old. The Hotline Analyst immediately determined that it was illegal under Irish law, and gathered the necessary technical information which would ultimately be used to trace and identify the specific ISP connection used by the alleged perpetrator.

The information was then transmitted by the Irish Hotline to our Bulgarian counterparts. This aided the Bulgarian Police Cybercrime Unit in locating and downloading the particular video, classifying it as illegal and requesting log-files from the relevant Internet Service Provider. As the activity was occurring on a service distributing dynamic IP addresses to the customers, the details provided by the Irish Hotline allowed to the Bulgarian Cybercrime Unit to trace the illegal activity to one specific IP address and identify the user as a 34 year old school teacher in the city of Plovdiv who had been teaching geography to pupils from 12 to 15 years of age.

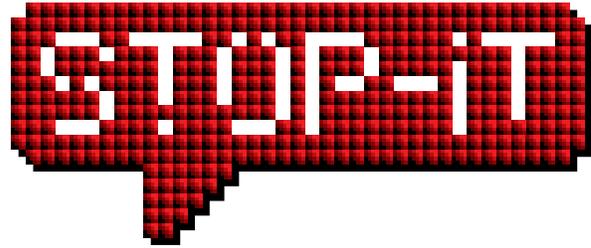
On the 12th May the Unit arrested the teacher and during the search in his home a large quantity of child pornography involving mainly pre-pubescent girls was discovered and confiscated as evidence. He was charged with possession and distribution of child pornography. This case shows how effective international cooperation between INHOPE Hotlines, Police and ISPs can be in tackling online distribution of child sexual abuse content. This arrest resulted specifically from the police investigation initiated by this report. These cases show how effective international cooperation between INHOPE Hotlines, Police and ISPs can be in tackling online distribution of child sexual abuse content.

## SAVE THE CHILDREN ITALY

Italy

[www.stop-it.it](http://www.stop-it.it)

+39 06 4807001



Save the Children is the world's largest international, independent organization working to promote and defend children's rights. Present in over 120 countries around the world, it is made up by a network of 30 national organizations and one international coordinating office (Save the Children International). Save the Children works in the field of humanitarian aid and in medium-long term assistance, wherever the organization recognizes that its own intervention can bring durable changes to children's lives today.

Save the Children Italy came into existence at the end of 1998 and became a member of INHOPE in 2003. In addition to online child sexual abuse, is currently managing projects in the following areas: child participation, child discrimination, child abuse and maltreatment, separated children, children on the move, child trafficking, child poverty. Regarding online child sexual abuse, Save the Children has been running the Stop-It Hotline since 2001, which provides an online facility [www.stop-it.it](http://www.stop-it.it), to general public for reporting online child sexual abuse material.

The Hotline works closely with relevant law enforcement agencies, the internet industry, government/policy makers, social service organizations, school/community groups and civilians to ensure effective measures are taken to prevent online child sexual abuse, to identify child victims and to guarantee that proper support is provided to them.

The hotline receives reports from the public via an online reporting form and email. When the hotline receives reports, they are forwarded to law enforcement for further processing and analysis. In 2013, Stop-It forwarded over 3,600 reports to the relevant law enforcement agency; during 2014 it went through a technical renewal and started its work again in early 2015.



## TELEFONO AZZURRO

Italy

[www.azzurro.it](http://www.azzurro.it)

[ufficio.presidenza@azzurro.it](mailto:ufficio.presidenza@azzurro.it)

An ongoing program developed by the Italian Safer Internet Centre (SIC), and co-founded by the European Commission, “Generazioni Connesse” (“Connected Generations”), assumes both roles of awareness center and “hotline coordinator in Italy. The focus of this program is to carry out awareness-raising activities by operating a national helpline and two selected partner hotlines. One of the hotlines enrolled by the SIC in cooperation of the specific aims of the project against child sexual abuse material is the SOS il Telefono Azzurro ONLUS hotline.

SOS il Telefono Azzurro was established as part of the “Generazioni Connesse” project in 2003 and became a member of INHOPE in 2013. They work actively with law enforcement, industry, social services and civilians to foster total respect for the rights of children and adolescents by promoting their potential growth and protecting them from abuse and violence that could threaten their well-being and their successful development and efficacious adjustment. To help achieve this mission, the hotline receives reports regarding possible online child sexual abuse material as well as, but not limited to, SPAM, adult pornography and suicide.

The hotline receives reports in several different ways: online reporting form, email and by telephone. Reports about CSAM come from the public and other INHOPE member countries. In general, these methods of reporting are publically available and user-friendly. In addition to reports regarding possible online child sexual abuse material, the hotline also offers other services aimed to alert or inform internet safety awareness to the general public, researchers, policy developers and victims or at-risk individuals.

When analysts receive the reports, they attempt to trace a geographical hosting location for the material. If the material is hosted in Italy, the report is forwarded to law enforcement. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country’s hotline. In 2014, SOS il Telefono Azzurro ONLUS received and forwarded 2,813 reports to law enforcement and/or INHOPE, of which approximately 88% were regarding CSAM. Furthermore, between when the hotline started receiving reports about CSAM in 2005 and the end of 2014, SOS il Telefono Azzurro ONLUS received and forward 16,844 total reports regarding potential CSAM.

SOS il Telefono Azzurro ONLUS plays a vital role in the protection of children from sexual exploitation, as evidenced by the hotline’s commitment to awareness raising activities, such as developing “safety laboratories” at high schools and sustaining an online awareness campaign

*(continued from previous page)*

via “recommendations about youth safety”. In addition, the hotline is also active within the INHOPE organization by attending the General Assemblies, participating in study exchanges and joining INHOPE webinars.



## INTERNET HOTLINE CENTER JAPAN

Japan  
[www.internethotline.jp](http://www.internethotline.jp)

A project under contract from the National Police Agency, the Internet Hotline Center (IHC) is an online hotline for the public in Japan that serves as a mechanism for anonymously reporting illegal or harmful information. With the information received from internet users, the Hotline is charged with several tasks, including informing the police, notifying industry of illegal and/or harmful material on their websites, informing related government and non-government institutions and handling online child sexual abuse material through international cooperation.

IHC was established within the non-profit organization, Internet Association Japan (IAJ), in 2006 and became a member of INHOPE in 2007. IHC works closely with law enforcement, the internet industry and government/policy makers to accomplish their mission and deliver their services. In addition to the hotline for processing reports about illegal or harmful information, the hotline also offers additional services related to community outreach and internet safety awareness, research on internet trends and technology and a safety helpline for children.

The hotline receives reports from the public as well as INHOPE member countries. Reports are received primarily through their online reporting form. In addition to possible online child sexual abuse material, the hotline receives reports regarding a variety of illegal and harmful information, including, but not limited to illegal drugs, adult pornography, group suicide, extreme violence and the buying and selling of human organs.

When reports are received at the hotline, analysts classify the reports based on their operational guideline and determine a geographical hosting location for the content. If content is hosted in Japan, law enforcement is notified. Then, when instructed by law enforcement, the hotline notifies industry to delete the content. If child sexual abuse material content is hosted in an INHOPE member country, the report is forwarded via INHOPE to the appropriate INHOPE member country. In addition, the hotline also provides a list of URLs that include child sexual abuse material to an external organization responsible for blocking those sites.

IHC has received 150,352 reports in 2014, of which 1,452 were regarding child sexual abuse material, and over 1,218,000 total reports between the time it was established and the end of 2014. IHC plays a vital role in the protection of children from sexual exploitation, as evidenced by the following highlight: IHC is a leading national Internet hotline staffed with 17 experienced analysts and 2 skilled managers (as of April 2015) who are committed to helping law enforcement conduct quality investigations and industry make a safer Internet environment

*(continued from previous page)*

by fast and effective responses to the reports. IHC also tries to be flexible with the change of criminal trends and social movements and adapts to these trends in order to tackle a varying range of online crime.



## INTERNET ASSOCIATION OF KAZAKHSTAN

Kazakhstan  
www.safekaznet.kz  
report@iak.kz  
+7 727 272 05 61

A program of the Internet Association of Kazakhstan, the safekaznet.kz hotline was established as a public mechanism for reporting online content that contains offensive and defamatory images, videos, comments or other materials related to pornography, drugs, violence, propaganda of cruelty, extremism and terrorism by means of public action.

Established in 2010, and currently an INHOPE foundation member, the safekaznet.kz hotline is a non-profit organization that works actively with the internet industry, law enforcement, government/policy makers and social services to deliver their services. In addition to receiving reports, the hotline offers other services related to community outreach and internet safety awareness and research/policy development.

The hotline receives reports via their online reporting form and through email. Reports come in from a variety of sources, including the public, law enforcement and INHOPE member countries. In addition to possible online child sexual abuse material, the hotline receives reports including, but not limited to, racism/hate speech, alcohol/tobacco/drugs, suicide, bullying and extreme violence/threats of violence.

When reports are received by the hotline, analysts review the material and attempt to identify the geographic hosting location for the material. If hosted in Kazakhstan, the reports are forwarded directly to the prosecutor's office and the hotline will notify the appropriate online hosting company of illegal/harmful content on their site. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline. In 2014, the safekaznet.kz hotline received 2,088 reports, of which 10 were regarding online child sexual abuse material.

**DROSSINTERNETS.LV**

Latvia

[www.drossinternets.lv](http://www.drossinternets.lv)[zinojumi@drossinternets.lv](mailto:zinojumi@drossinternets.lv)**DROSS  
INTERNETS.LV**

Coordinated by the Latvian Internet Association, Drossinternets.lv was established as part of the Net-Safe Latvia Safer Internet Centre as a public mechanism to report illegal material online. Net-Safe Latvia Safer Internet Centre is the national contact point for the European Union's *Connecting Europe Facility* (CEF) program, Insafe, which is a network devoted to coordinating internet safety awareness in Europe.

Established in 2007 and a member of INHOPE in 2008, Drossinternets.lv works actively with law enforcement, the internet industry, government/policy makers and civilians to combat illegal online content. In addition to receiving reports, the hotline also offers additional services related to community outreach and internet safety awareness and advocate/law enforcement training.

The hotline receives reports via their online reporting form and through email. Reports are made by members of the public and INHOPE member countries and then assessed by hotline analysts. In addition to combating online child sexual abuse material, the hotline also receives reports about, and attempts to combat, racism/hate speech, adult pornography, bullying, fraud, and extreme violence/threats of extreme violence.

When Drossinternets receives a report, analysts review the reported material and attempt to identify a geographic hosting location for the material. If the material is hosted in Latvia, the report will be forwarded to law enforcement and the appropriate hosting provider will be notified to remove the content. If the content is hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline.

In 2014, Drossinternets.lv received 818 reports regarding potentially harmful content on the Internet, 315 of which were regarding child sexual abuse material. Furthermore, between its inception in 2007 and the end of 2014, the hotline has received a total of 3,557 reports, of which 898 were regarding child sexual abuse material.



## SAFER INTERNET LT

Lithuania

[www.draugiskasinternetas.lt](http://www.draugiskasinternetas.lt)

[hotline@esaugumas.lt](mailto:hotline@esaugumas.lt)

The Safer Internet LT hotline, established by the Communications Regulatory Authority of the Republic of Lithuania (RRT) and co-funded by the European Union within the framework of the Safer Internet Program, serves as a reporting mechanism for potentially illegal or harmful material on the Internet. The RRT is a national institution which oversees the communications sector in Lithuania. In particular, the organization strives to ensure the information and communications technology in Lithuania is high quality, progressive, and safe.

The Safer Internet LT hotline was established in 2007. In addition to reports on potential child sexual abuse material, the hotline also receives reports which include concerns of racism/hate speech, adult pornography, and bullying. Reports are made to the hotline via an online reporting form and email.

Upon receipt of a report, a hotline analyst assesses the material in question and attempts to locate where the illegal content is hosted. If the content is on a Lithuanian server, the hotline partners with local law enforcement and the electronic service provider in question to ensure a prompt investigation and removal of the illegal content. If the material is hosted internationally, a report is forwarded via the INHOPE network of global hotlines to the representative hotline where the content is located.

Since the hotline's inception, it has received (until 1<sup>st</sup> April 2015) 4,667 reports of potentially illegal material and in 2013 alone, the hotline received 650 reports. In 2014 the hotline received 733 reports, from which CSAM was determined in 124 cases (19 reports were sent to the Lithuanian police and 105 reports were sent to the other hotlines through INHOPE Report Management System).

The Safer Internet LT Hotline is part of the Lithuanian Safer Internet Centre and is an active member of INHOPE since May 2008.

## BEE SECURE STOPLINE

Luxembourg  
 www.stopline.bee-secure.lu  
 kjt@bee-secure.lu



Operated by the Kanner-JugendTelefon (Luxembourgish National Child Helpline), a consortium partner of the Safer Internet Centre along with the Service National de la Jeunesse and SMILE g.i.e (“Security made in Lëtzebuerg”), the BEE SECURE Stopleveline was established as a mechanism for the public to report on illegal content encountered on the internet. Initially called LISA Stopleveline, the hotline’s name was changed to better reflect their integration with the activities of the Luxembourg Safer Internet Centre BEE SECURE which, in addition to the hotline, consists of awareness raising and the BEE SECURE Helpline.

Established in 2008 and a member of INHOPE in the same year, the BEE SECURE Stopleveline actively collaborates with law enforcement, the internet industry, the government/policy makers, social service organizations and civilians to deliver their services. In addition to receiving reports, the hotline also offers services related to community outreach and internet safety awareness.

The hotline receives reports through their online reporting form. Reports are made to the hotline by law enforcement, the public and INHOPE member countries. In addition to possible online child sexual abuse material, the hotline receives reports including, but not limited to, racism/hate speech discrimination and terrorist content.

When reports are received by the hotline, analysts review the material and attempt to determine the geographical hosting location. If hosted in Luxembourg, analysts will forward the report to law enforcement and then, upon approval from law enforcement, notify hosting companies to have the content removed. If the material is hosted internationally, the report is forwarded via INHOPE to the appropriate member country’s hotline and to law enforcement.

In 2014, the BEE SECURE Stopleveline received 1,159 reports regarding potential child sexual abuse material, of which 683 were determined to be illegal by the hotline analysts and forwarded to law enforcement according to the hotline’s operational procedures.

BEE SECURE Stopleveline plays a vital role in the protection of children from sexual exploitation, as evidenced by “Operation Carol” in 2012. In this sequence of events, a report was made to the hotline regarding child sexual abuse material which was subsequently forwarded to law enforcement authorities. After an investigation, that report ultimately led to the arrest of hundreds of people in 141 countries.



## CHILD WEB ALERT

Malta

[www.childwebalert.gov.mt](http://www.childwebalert.gov.mt)

Established by Agenzija Appogg, Malta's National Agency for the protection of children, and a program of Malta's BeSmartOnline! project, the Child Web Alert Hotline was established to serve as a mechanism for reporting internet abuse. In addition to operating the hotline, the aims of the BeSmartOnline! project are to raise awareness; educate minors, caregivers and educators on the safe use of the internet; run a helpline on online abuse issues and; support victims.

Established in 2010 and a member of INHOPE in 2011, Child Web Alert collaborates with law enforcement, other government/policy makers, social service organizations and civilians to disrupt the availability of child sexual abuse material online, protect child victims of sexual abuse and prevent internet users from accidentally stumbling across child sexual abuse material. In addition to receiving reports, the hotline also offers additional services related to community outreach and internet safety awareness, research/policy development and direct victim services.

The hotline receives reports via their online reporting form, and by telephone or email. Reports are made to the hotline by members of the public and INHOPE member countries. In addition to possible online child sexual abuse material, the hotline receives reports regarding, but not limited to, racism/hate speech, pro-anorexia, bullying and suicide/self-harm.

When reports are received by the hotline, the content is analyzed and a geographic hosting location is determined for illegal material. If hosted in Malta, the report is forward to law enforcement. If hosted internationally, the report is forwarded to law enforcement and also to the appropriate member country's hotline via INHOPE.

In 2014, Child Web Alert received 168 reports regarding potential child sexual abuse material and, between the time of the hotline's inception in 2010 and the end of 2014, the hotline has received a total of 620 reports. Child Web Alert plays a vital role in the protection of children from sexual exploitation, as evidenced by the following hotline highlight: Their agency runs both the hotline and the internet helpline where people can contact us regarding online abuse. Our helpline supports the victims with one to one counselling sessions especially in sexting cases and cyberbullying. The hotline works directly with the Child Protection Service within Agenzija Appogg, so if a local child is being abused, immediate support can be provided by the child protection Agency.

## ALIANZA POR LA SEGURIDAD

### INTERNET

Mexico

[www.asi-mexico.org](http://www.asi-mexico.org)



The Alianza por la Seguridad Internet (ASI) is a non-profit working to “provide guidance for the safe and responsible use of the Internet, and receive reports of illegal content found on the Internet by users in the country”. ASI works in partnership with law enforcement, the Internet and communications industry, community organizations and policy makers.

Since 2009 ASI has operated a hotline that serves as a reporting point for Internet users who have come across potentially illegal material online. In addition to possible child sexual exploitation material, the hotline receives reports concerning SPAM, gambling, substance abuse, adult pornography, pro-anorexia, bullying, and fraud. Reports are made to the hotline via email and online reporting form. Upon receipt of a report, hotline staff review the reported content and forward reports of illegal material to Mexican law enforcement for further investigation.

ASI understands the importance of partnering with both the public and private sectors and in 2015 reached an agreement with GSMA and the Mexican National Telecom Association (ANATEL) to improve consumer protection. The “We Care” Campaign focuses on several areas of public concern, one of which is child protection. In support of this mission, GSMA and ANATEL will support mobile reporting of potentially illegal material to the ASI website.

The hotline received approximately 7,600 reports in 2014 across all reporting categories and has received over 36,000 reports since its launch in 2009.



## LINEA CIUDADANO

Mexico

[www.consejociudadanodf.org.mx](http://www.consejociudadanodf.org.mx)

[contacto@consejociudadanodf.org.mx](mailto:contacto@consejociudadanodf.org.mx)

The Consejo Ciudadano is a non-profit, civil society organization located in Mexico City, with a presence in several states of the Mexican Republic. The Consejo Ciudadano is responsible for monitoring and supervising the actions of city officials. Additionally, the Consejo Ciudadano's goals are aimed at promoting programs to address specific problems associated with public safety, law enforcement, and civic culture.

The Consejo Ciudadano's philosophy is to be more proactive and action-oriented. The strategies employed by the Consejo Ciudadano were built based on what is called a "PPC (public - private - civil) model". In this way, members of the community have been encouraged to participate and civic responsibility has been engendered as a result.

Since 2007, the Consejo Ciudadano has operated the Linea Ciudadano (5533-5533), a reporting mechanism for members of the public to report concerns regarding public safety in a way that is simple, confidential, and effective. Since its inception the Linea Ciudadano has resulted in several successful outcomes in cases of sextortion, human trafficking, and bullying.

Today, reports can be made to the hotline via email, telephone, text message, or social networking sites, such as Twitter and Facebook. Upon receipt of a report, a hotline analyst reviews the content and forwards the report to the appropriate authorities. It is of importance to note that in February of this year, the Consejo Ciudadano developed the app NomásXT, which is the first of its kind to aid in the prevention of sextortion.

The hotline is actively developing its reporting process for instances of online child sexual exploitation material. In addition to receiving reports of child sexual abuse, as part of its commitment to INHOPE, the Consejo Ciudadano is currently pursuing full membership in the network.

## MELDPUNT KINDERPORNO

The Netherlands  
[www.meldpunt-kinderporno.nl](http://www.meldpunt-kinderporno.nl)  
[info@meldpunt-kinderporno.nl](mailto:info@meldpunt-kinderporno.nl)



An independent private foundation to combat child pornography on the internet, the Meldpunt Kinderporno hotline was officially opened by the Ministry of Justice at the initiative of internet providers and individual internet users. The aim of this hotline was to contribute to the reduction of the distribution of child abuse images online.

Established in 1996 and an INHOPE member the same year, Meldpunt Kinderporno is a non-profit hotline that actively partners with law enforcement, the internet industry, government/policy makers and civilians to deliver their services. In addition to the receiving reports, the hotline offers a variety of other services related to community outreach and internet safety awareness, research/policy development and direct victim services.

The hotline receives reports via their online reporting form, and by email and telephone. Reports are made to the hotline by the public, law enforcement, the internet industry and INHOPE member countries and then assessed by hotline analysts. The hotline has two criteria by which content must meet in order to be processed by the hotline: the content must be a pictorial representation of a sexual act involving someone under the age of 18 and there must be public distribution of that content via the internet. If reports do not meet these criteria, they will not be processed by the hotline.

When the hotline receives a report, analysts review the reported material to determine if it meets the hotline's criteria and then the content is assessed to determine the geographic hosting location. If hosted in domestically, the hotline will notify the hosting provider so that the content will be removed and the reports are sometimes forwarded to law enforcement as well. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline.

In 2014, the Meldpunt Kinderporno hotline received 28,960 reports and, between the time of its inception in 1996 and the end of 2014, has received a total of 163,018 reports.

The hotline plays a vital role in the protection of children from sexual exploitation, and has a strong focus on international cooperation. According to the hotline:

“The Netherlands is very popular among foreign suppliers of data center services. The appeal to foreign investors can be explained by the good telecommunications infrastructure, the reliable energy supply,

*(continued from previous page)*

the strategic location and the innovative character of the Netherlands as a ‘data center country’, among other factors. Being popular has its downsides, however. For example, the hosting of illegal content. The reports that Meldpunt receives increase every year and 60% of this year’s reports were related to illegal material, which is a high percentage. To be able to do our job and invest in the future we can use all the help we can get. It’s not only about getting illegal content removed, but getting to the source and working together internationally is necessary to really tackle this problem.”

## THE ORB

New Zealand

[www.theorb.org.nz](http://www.theorb.org.nz)

[queries@netsafe.org.nz](mailto:queries@netsafe.org.nz)



An initiative of NetSafe, The Orb is an online reporting mechanism for potentially illegal material on the Internet. NetSafe, founded in 1998, endeavors to ensure the public's safety when online. In addition to hotline services, NetSafe offers community outreach and Internet safety initiatives and contributes to research and policy development surrounding safe use of the Internet. NetSafe is a multi-stakeholder, non-profit organization working in partnership with law enforcement, families, the Internet services industry, community organizations, and area policy makers.

The Orb became operational in 2010. The Orb acts as the public interface for reports regarding all varieties of online criminal behavior. In addition to possible child sexual abuse material, the hotline receives reports concerning SPAM, adult pornography, pro-anorexia/self-harm, bullying, and fraud. The Orb in turns refers reports to the appropriate organization for further action. Reports can be made via telephone, email, or online reporting form. In instances of potential child sexual abuse material online, the hotline does not have the legal ability to review the reported content and all reports are forwarded directly to law enforcement via ECPAT-New Zealand for further investigation.

Since its launch, The Orb has received 15,529 reports and in 2014 alone received approximately 5,200 reports.

NetSafe is an active member in the INHOPE global network of hotlines.

NetSafe has graciously offered the following case study of the important work done by the hotline:

A 13 year old girl was befriended on social media and following a period of grooming was persuaded to upload sexual videos to a Vine account, a service owned by Twitter. The new friend then changed the password for the account and tried to blackmail the child into creating more videos. A worried parent contacted Vine but received only an automated reply. After the parent talked with the school, it was discovered that other students had seen the content. The parent contacted OCEANZ and NetSafe and although accepting they may remain online forever, wanted the videos removed from Vine. Removing the harmful content from commonly accessed spaces reduces the stress on the victim. Therefore, NetSafe contacted Twitter staff via a US partner. The Vine safety team responded immediately. They removed the videos and reported the offender to the FBI's National Centre for Missing and Exploited Children (NCMEC).



## SEGUROS EN INTERNET

Peru

[www.seguroseninternet.org](http://www.seguroseninternet.org)

+51 1 434 3604

A program of the non-profit organization, Peruvian Network against Child Pornography, Seguros en Internet was established to help fight their mission, which is to eradicate the networks of producers, distributors and consumers of child pornography, especially on the internet and, in addition, to fight against child sexual exploitation and trafficking of babies.

Established in 2008, and currently a foundation member of INHOPE, Seguros en Internet actively partners with law enforcement, the internet industry, government/policy makers, social service organizations and civilians to deliver their services. In addition to receiving and processing reports, the hotline offers a variety of other services related to community outreach and internet safety awareness, research/policy development, direct victim services and advocate/law enforcement training.

The hotline receives reports via their online reporting form as well as by email. Reports are made to the hotline by members of the public as well as INHOPE member countries. In addition to online child sexual abuse material, the hotline handles reports related to grooming, ads for exploitation or child sex tourism, bullying and cyberbullying, racism/hate speech, pro-anorexia and other harmful content.

When reports are received at the hotline, analysts review the reports and attempt to identify the geographic hosting location for the material. If hosted domestically, the report is forwarded to law enforcement and hosting providers are notified so that content will be removed. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline.

In 2014, Seguros en Internet received 98 reports, of which 82 were related to child sexual abuse material. Between the time of the hotline's inception in 2008 and the end of 2014, they have received a total of 353 reports, of which 311 were related to child sexual abuse material.

Seguros en Internet plays a vital role in the protection of children from sexual exploitation, as evidenced by their commitment to handling reports under changing trends. For example, the hotline has recently received more reports related to sexual abuse cases and grooming—most of which are related to the misuse of public profiles and social networks.

DYZURNET.PL

Poland

www.dyzurnet.pl

+48 22 5231 050

dyzurnet  pl

Acting within the framework of the Research and Academic Computer Network, Dyzurnet.pl hotline was established as a public mechanism to report illegal content on the internet that involves child abuse, threatens children's safety, or promotes xenophobia and racism. The hotline's activities are regulated by Polish law and based on domestic and international cooperation.

Established in 2005 and a member of INHOPE the same year, Dyzurnet.pl actively partners with law enforcement, the internet industry, government/policy makers and civilians to deliver their services. In addition to receiving and processing reports, the hotline offers other services related to community outreach and internet safety awareness, research/policy development and advocate/law enforcement training.

The hotline receives reports via their online reporting form and by email and telephone. Reports are made to the hotline by the public as well as INHOPE member countries. In addition to possible online child sexual abuse material, the hotline receives reports regarding racism/hate speech, adult pornography, pro-anorexia, bullying, suicide and other content considered by Internet users as harmful.

When the hotline receives reports, they are assessed by analysts based on their content and a geographical hosting location for the material is identified. If hosted in Poland, law enforcement is alerted and, only then, the hosting provider will be notified to remove the content from the internet. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline.

In 2014, Dyzurnet.pl received 11,063 reports, of which 9,117 were regarding potential CSAM and 1,395 were confirmed as CSAM. Furthermore, between the time of the hotline's inception in 2005 and the end of 2014, the hotline has received 44,893 total reports, of which 31,130 were regarding potential CSAM and 8,590 were confirmed as CSAM.



LINHA ALERTA

Portugal

[www.linhaalerta.internetsegura.pt](http://www.linhaalerta.internetsegura.pt)

[report@linhaalerta.internetsegura.pt](mailto:report@linhaalerta.internetsegura.pt)

+351 218440126

A program of the Internet Segura project, Linha Alerta was developed as a non-profit public mechanism for reporting illegal content online, such as child abuse images, incitement to violence and incitement to racist content, so that it can be blocked and disseminators can be prosecuted in an effective way. The Internet Segura project includes two components, the Linha Alerta hotline and an awareness node, and was co-funded by the European Commission under the Safer Internet Plus Program.

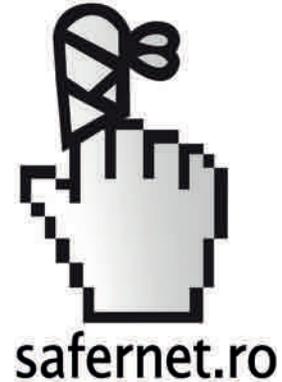
Established in 2006 and a member of INHOPE in 2007, Linha Alerta actively partners with law enforcement, the internet industry and civilians to deliver their services. In addition to receiving and processing reports, the hotline also engages in activities related to community outreach and internet safety awareness.

The hotline receives reports via their online reporting form, by email and by telephone. Reports are received by members of the public as well as transferred through INHOPE from a member country. In addition to possible online child sexual abuse material, the hotline receives reports regarding racism/hate speech, violence, terrorist propaganda and adult pornography.

When hotline analysts receive the reports, the content is assessed and a geographical location for the content is identified. If hosted in Portugal, law enforcement is notified and the hosting provider will be notified to remove the content. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline. In 2013 alone, Linha Alerta received over 2,100 reports.

## SAFERNET.RO

Romania  
www.safernet.ro  
contact@safernet.ro  
+40213103116



The Safernet.ro hotline is a program of the non-profit organization, the Romanian Center for Missing and Exploited Children-FOCUS. The mission of the Center implies both prevention and participation in solving cases of missing, abducted and sexually exploited children. To help with this mission, the Safernet.ro hotline was established as a civil contact point, which receives and processes reports referring to materials on the Internet of an illegal or harmful nature for children.

The Safernet.ro hotline was established in 2009 and became a member of INHOPE in 2010. The hotline actively partners with law enforcement, the internet industry, government/policy makers, social service organizations and civilians to provide their services.

The hotline receives reports via their online reporting form, email, telephone, fax and smartphone app. Their reports come from members of the public as well as by INHOPE members. In addition to possible online child sexual abuse material, the hotline receives reports regarding a variety of issues, including SPAM, racism/hate speech, adult pornography, drugs and child trafficking.

When reports are made to the hotline, analysts assess the content and attempt to determine the geographic hosting location for the material. If hosted in Romania, local law enforcement will be alerted if the content is illegal, so as not to interfere with any investigation by having the content removed, and the hosting provider will only be notified if the content is legal but harmful so that it can be taken off the Internet. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline.

In 2014, Safernet.ro received 1,400 reports, of which 280 were confirmed as CSAM. Furthermore, between the time between the hotline's inception in 2009 and the end of 2014, the hotline has received over 4,500 total reports, over 1,000 of which were confirmed as CSAM. Safernet.ro plays a vital role in the protection of children from sexual exploitation, as evidenced by their great relations with partners from the Cybercrime department of the Romanian Police and with local child protection authorities—many of the hotline's reports that are sent to the police become strong cases and investigations for combating CSAM in Romania.



## FRIENDLY RUNET FOUNDATION

Russian Federation  
[www.friendlyrunet.ru](http://www.friendlyrunet.ru)  
[info@friendlyrunet.ru](mailto:info@friendlyrunet.ru)

A core function of the Friendly Runet Foundation is operation of a hotline allowing Internet users to report instances of possible child sexual abuse material. The Friendly Runet Foundation strives to make the Internet a safer place. In addition to hotline services, the Foundation works closely with Internet Service Providers, law enforcement, and government to support issue based research and encourage relevant and impactful policy development.

The hotline was established in 2009 and strives to disrupt the distribution of child sexual abuse material online. Members of the public may make reports to the hotline via email or using the hotline's online reporting form. Upon receipt of a report, a hotline analyst will assess the content and attempt to identify the country hosting illegal content. If a Russian company, Friendly Runet will alert law enforcement for investigative purposes and the relevant hosting company to ensure prompt removal of the media. If hosted internationally, a report is forwarded via the INHOPE network to a hotline in the hosting country.

Since its launch in 2009, the hotline has received more than 177,000 reports and in 2014 alone received close to 38,000 reports.

Friendly Runet Foundation is an active member of the INHOPE association of global hotlines.

## SAFER INTERNET CENTRE-RUSSIA

Russian Federation  
www.nedopusti.ru  
hotline@nedopusti.ru

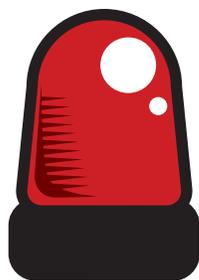


The Safer Internet Centre-Russia hotline is a reporting mechanism for instances of illegal or harmful material on the Internet, including child sexual abuse material. In 2012 the Safer Internet Centre – Russia became the base for the emerging Russian National Centre for Missing & Exploited Children. The Russian National Centre for Missing & Exploited Children, operated by non-profit organization ROCIT, works with support from law enforcement, the Internet and communications industry, and government policy makers. In addition to hotline services, the organization offers outreach and training to communities, families, and child protection professionals, direct victim support, victim identification, and contributes to issue based research and policy development.

Launched in 2008, the hotline is the first and oldest Russian hotline on illegal content and is a “meeting point” for cooperation of Internet-users, industry, government and law enforcement in combating illegal content. In addition to reports of possible child sexual abuse material, the hotline performs checks on possible missing children and receives concerns about racism/hate speech, bullying, and substance abuse. Reports are made via online reporting form or, rarely, via email. Upon receipt of a report, hotline staff reviews the reported media and attempt to locate in which country the material is hosted. If a Russian hosting company, a report is made available to law enforcement for possible investigation and the hosting company is alerted to ensure swift removal of the content. If hosted internationally, the hotline utilizes the INHOPE network to identify a hotline for further action and forwards the complaint.

Since its inception in 2008, the hotline has received more than 53,000 reports regarding possible child sexual abuse material and in 2014 alone received almost 16,000 reports.

The Russian Safer Internet Centre is part of the Russian National Centre for Missing & Exploited Children and has been a member of INHOPE since 2009.



**NET PATROLA**  
www.netpatrola.rs

**NET PATROLA**  
Serbia  
www.netpartrola.rs  
office@netpatrola.rs

A member of the Safer Internet Hotlines, Net Patrola is a non-profit that was established to allow the reporting and processing of submissions of illegal or harmful content on the internet in Serbia. Established in 2013 and a member of INHOPE in the same year, the main priority of the hotline work is countering the spread of child sexual abuse images and physical and psychological attacks against children.

Net Patrola actively works with members of law enforcement, the internet industry, government/policy makers and civilians to deliver their services. In addition to receiving and processing reports, the hotline offers additional services related to community outreach and internet safety awareness and research/policy development.

The hotline receives reports via their online reporting form and by email. Reports are made to the hotline by members of the public and also by INHOPE member countries. In addition to reports regarding possible online child sexual abuse images, the hotline receives reports regarding adult impersonation of a minor engaged in sexual molestation or pornography, material that promotes the commitment of psychological or physical violence over minors, racism/hate speech and bullying.

When reports are received by Net Patrola, analysts review the material and attempt to determine the geographical hosting location of the material. If hosted in Serbia, analysts alert the appropriate agency, which may include law enforcement and hosting providers. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline.

In 2014, Net Patrola received 313 reports related to child sexual abuse material, an increase from 22 reports in 2013. Moreover, between the time of the hotline's inception in 2013 and the end of 2014, they received almost 2,000 total reports. Net Patrola plays a vital role in the protection of children from sexual exploitation, as evidenced by their excellent cooperation with law enforcement and their educational and awareness raising efforts about digital safety. Through their workshops in schools, they have addressed more than 15,000 people, which have included parents and staff, but which primarily included children aged 7-18.

## STOPLINE.SK

Slovakia

[www.stopline.sk](http://www.stopline.sk)

[stopline@stopline.sk](mailto:stopline@stopline.sk)



Stopline.sk is a program of the Slovak Safer Internet Centre, a non-profit organization that is co-funded by the European Union within the Safer Internet Program. Among other goals, the organization aims to raise awareness of the public to behave responsibly when using the internet and other communication technologies. In addition to the Stopline.sk hotline, the Centre consists of two other main components, a helpline and an awareness node.

Stopline.sk was established in 2010 and became a member of INHOPE in the same year. The hotline actively partners with law enforcement, the internet industry, government/policy makers and civilians to deliver their message and services. In addition to receiving and processing reports, the hotline also related to community outreach and internet safety awareness, research/policy development and victim identification.

The hotline receives reports via their online reporting form and by email. Reports are made to the hotline by members of the public as well as via INHOPE from member countries. In addition to possible online child sexual abuse material, the hotline receives, but is not limited to, reports regarding racism/hate speech and bullying.

When reports are received at Stopline.sk, analysts assess the content to determine if it is illegal material. If so, and if it is hosted in Slovakia, analysts will alert law enforcement officials. If hosted internationally, analysts will forward the report to the appropriate hotline via the INHOPE network. In 2013 alone, the hotline received 3,600 reports.



SPLETNO OKO  
Slovenia  
[www.spletno-oko.si](http://www.spletno-oko.si)  
[info@spletno-oko.si](mailto:info@spletno-oko.si)

A program of the Safer Internet Centre Slovenia, the Spletno Oko hotline is one of the Centre's three components along with the Awareness Centre and Helpline. The Safer Internet Centre was initiated by the European Union and is a national project promoting and ensuring a better internet for kids. To help accomplish the goals of the Centre, the Spletno Oko hotline functions as a mechanism for internet users to report hate speech and child sexual abuse images.

The Spletno Oko hotline was established in 2007 and became a member of INHOPE in 2011. The hotline actively partners with academia, law enforcement, the internet industry, government/policy makers, social service organizations and civilians to accomplish their mission and deliver their services. In addition to receiving and processing reports, the hotline offers additional services related to community outreach and internet safety awareness, research/policy development, direct victim services and advocate/law enforcement training.

The hotline receives reports via their online website and by email. Reports are made to the hotline by members of the public as well as INHOPE member countries. In addition to possible online child sexual abuse material, the hotline only handles reports regarding hate speech. In the circumstance that reports come in regarding other topics, such as adult pornography, SPAM, cyberbullying, incitement to inappropriate behavior, threats toward an individual, grooming and abuses on social networking sites, the hotline provides users with tips on how to deal with such situations.

When reports are received, analysts assess the content and determine a geographic hosting location for the material. If it is hosted in Slovenia, the appropriate agencies will be notified, such as law enforcement who, in turn, will notify hosting providers of content on their sites. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline.

Between the time of the hotline's inception in 2007 and the end of 2014, the hotline received 4,350 total reports. In 2014 alone, Spletno Oko received 521 reports regarding child sexual abuse material and forwarded 72 of those reports to the police for further investigation.

## FILM AND PUBLICATION BOARD INTERNET HOTLINE

South Africa  
www.fpbprochild.org.za  
clientsupport@fpb.org.za  
+27 (0) 12 003 1400



An initiative of the Film and Publication Board in South Africa, the Internet Hotline is a government service that allows the public to make online reports regarding any images they suspect to be child pornography or sexual abuse images. The Board was established by an Act of parliament, the Films and Publications Act 65, 1996, which regulates the creation, production and distribution of films, games and certain publications with the aim of protecting children from exposure to inappropriate material and to make the exploitation of children in the creation of child pornography punishable.

The Internet Hotline became operational in 2009 and a member of INHOPE in 2011. It was developed out of a mission to ensure efficient and effective consumer protection through regulation of media content to ensure protection of children, while empowering the public, especially children, through robust information sharing. To achieve this goal, the Internet Hotline actively partners with law enforcement, the internet industry, government/policy makers, social service organizations, school/community organizations and civilians to achieve their mission and deliver their services. In addition to receiving and processing reports, the hotline offers additional services related to community outreach and internet safety awareness, research/policy development, direct victim services and advocate/law enforcement training.

The hotline receives reports via their online reporting form, by email and by telephone. Reports are made to the hotline by law enforcement, the public and INHOPE member countries. In addition to possible online child sexual abuse material, the hotline receives reports regarding, but not limited to, child trafficking, drugs, racism/hate speech, adult pornography and bullying.

When reports are received, hotline analysts review the material and attempt to identify the geographic hosting location for the material. If hosted in South Africa, the report is forwarded to law enforcement. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline.

In 2014, the FPB Internet Hotline received 169 reports and, in the time between the hotline's inception in 2009 and the end of 2014, received a total of 1754 reports. The Hotline plays a vital role in the protection of children from sexual exploitation, including testifying in court in cases of child pornography.



## ILLEGAL AND HARMFUL INFORMATION REPORT CENTER

South Korea  
[www.singo.or.kr](http://www.singo.or.kr)  
[inhope@kocsc.or.kr](mailto:inhope@kocsc.or.kr)

The Korea Communications Standards Commission works to “ensure the public responsibility and fairness of broadcast contents and to cultivate a culture of safe Internet communications.” In support of this goal, the KCSC works closely with the law enforcement, the internet and communications industry, and policy makers.

Since its establishment in 2008, the Commission has dedicated itself to regulating harmful online materials through reports from the public in an effort to help promote a safe online environment. Direct victim services, Internet safety awareness training, research and policy development are offered by the Commission in addition to its regulation services. Along with reports of possible child sexual abuse material, the Commission receives reports about racism/hate speech, gambling, substance abuse, adult pornography, self-harm and national security issues.

Reports may be made to the Commission via on- and off-line reporting channels, including email, telephone, in person report and smartphone app. Upon the receipt of a report, the content is reviewed and the Commission attempts to locate in which country the material is being hosted. If the material is locally hosted in South Korea, the Commission partners with law enforcement and Internet Service Providers (ISPs) and content providers to ensure prompt removal of the material. If the material is hosted internationally, the report is made to INHOPE for transfer to a member hotline in that country or the Commission requests the local Internet Service Providers to block access to the concerned material. If the material is deemed illegal that may incur further harm, the KCSC informs relevant organizations for efficient investigations and actions.

The KCSC has reviewed approximately 516,702 cases of illegal and harmful materials received via individual complaints, related organizations and self-monitoring between 2008 and 2014, and requested corrective actions, such as removal and access blocking, against 467,195 of them. In 2014, approximately about 132,884 cases of illegal and harmful material, such as pornography, illegal gambling, sex trafficking and child sexual abuse.

The Korean Communications Standards Commission has been a member of the INHOPE community since 2005.

## ECPAT HOTLINE

Sweden

[www.ecpathotline.se](http://www.ecpathotline.se)

[info@ecpat.se](mailto:info@ecpat.se)



### **MOT BARNSEXHANDEL**

ECPAT Sweden (End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes) was established in 1996 to combat the commercial sexual exploitation of children. It is part of the larger global network, ECPAT International. The organization works closely with law enforcement, Internet Service Providers (ECPAT Sweden initiated the voluntary blocking cooperation between Swedish National Police and the ISPs in 2005), the travel industry and financial sector to achieve their mission. In addition to hotline services, ECPAT contributes to research and policy development, and works with advocacy to strengthen legislation in the CSEC field.

In 2005, ECPAT launched its Hotline for the reporting of online child sexual abuse material. Reports can be made to the hotline via email or online reporting form. Upon receipt of a report, the hotline assesses the material and attempts to trace the origin of the illegal content. If the material is hosted in Sweden, ECPAT partners with law enforcement and the hosting company, will quickly investigate illegal content and remove it from the web. ECPAT Sweden is also an active member in the INHOPE global association of hotlines and if the material originates outside of Sweden, a report is forwarded via the INHOPE network of hotlines for further review and action.

Since its launch in 2005, ECPAT has received approximately 50 000 unique reports. In 2014 ECPAT received 2 715 reports of possible online child sexual abuse material. During the first quarter of 2015, the number of reports tripled compared with the corresponding period 2014.

ECPAT Sweden's collaboration with telecom company Telenor has resulted in Telenor Safe Report, a bookmark available in all Telenor mobile devices (iPhone in March 2015, Android later in the spring) which enables the user to report suspected CSAM directly to ECPAT Hotline.



WEB547

Taiwan

[www.web547.org.tw](http://www.web547.org.tw)

[web547@ecpat.org.tw](mailto:web547@ecpat.org.tw)

A program of ECPAT – Taiwan, Web547 acts as a reporting mechanism for possibly illegal or harmful material, with particular focus on child sexual abuse material. Web547 means “no pornography on websites” as the Chinese pronunciation of “547” sounds like the Chinese words for “no pornography”. ECPAT –Taiwan is part of the larger international organization ECPAT International which focuses on commercial child exploitation. In addition to hotline services, ECPAT-Taiwan offers direct victim services, training to families, communities, and child protection professionals, and contributes to issue focused research and policy development.

Web547 became operational in 1999 as a reporting mechanism for members of the public who stumble across instances of Internet facilitated child sexual exploitation. In pursuit of their mission, the organization partners closely with law enforcement, the internet and communications industry, community members, and policy makers. Reports are made to the hotline via email, telephone, or online reporting form. Upon receipt of a complaint, the hotline reviews the reported media and attempts to identify the country in which the media is hosted. If the website is within Taiwan, Web547 partners with law enforcements and the electronic service provider to ensure a thorough investigation and prompt removal of the illegal material. If the website originates internationally, a referral is made via the INHOPE network for further action by a hotline in the hosting country.

In 2014, the hotline received 6,582 total reports, 912 of which were reported as potential CSAM.

Web547 is an active member in the international association of hotlines, INHOPE.

**THAIHOTLINE**

Thailand

[www.thaihotline.org](http://www.thaihotline.org)

A program of the Internet Foundation for the Development of Thailand, ThaiHotline is a non-profit that was established in as a channel for internet users to report illegal or harmful content they have found online in an attempt to reduce this content by obstructing the appearance of this type of content on the internet. The Foundation is a non-profit organization established in 2003 and aims to create a safe environment of internet usage with creatively utilizing of information technology.

Established in 2009 and currently an INHOPE Foundation member, the ThaiHotline actively partners with law enforcement, the internet industry, government/policy makers, schools/community organizations and civilians to accomplish their mission and deliver their services. In addition to processing reports, the hotline offers additional services related to community outreach and internet safety awareness as well as research/policy development.

The hotline receives reports via their online reporting form, by email and by telephone. Reports are made to the hotline by members of the public as well as INHOPE member countries. In addition to possible online child sexual abuse material, the hotline receives reports including, but not limited to, SPAM, prostitution, racism/hate speech, gambling, alcohol/tobacco/drugs, adult pornography, bullying, offenses against the royal family, national socialistic offenses, violations of privacy and information against social order.

When reports are made to the hotline, analysts review the material and attempt to determine a geographic hosting location for the material. If hosted by a Thai company, law enforcement will be alerted and the hosting provider will be notified to remove the content. If hosted internationally, the report is forwarded via INHOPE to the appropriate member country's hotline. In 2014, ThaiHotline received 3,208 reports, of which 528 were regarding potential CSAM. Furthermore, between the time of the hotline's inception in 2009 and the end of 2014, the hotline has received 24,196 total reports, of which 1,202 were regarding potential CSAM.

ThaiHotline plays a vital role in the protection of children from sexual exploitation, as evidenced by the hotline recently collaborating with the CRC Coalition Group, a child-rights based organization in Thailand aimed at improving children's quality of life regardless of sex, religion, age, nationality and ethnic origin, etc. Therefore, the ThaiHotline has more connections with stakeholders working to combat CSAM on the Internet in Thailand, such as their first priority, which is building a good mechanism for the legal processing of CSAM. In addition, ThaiHotline

*(continued from previous page)*

also got involved with the National Legal Research Group on sexually abused children, whose mission is to examine and implement best practices in combating child sexual abuse material on the Internet.

## IHBAR WEB

Turkey

[www.ihbarweb.org.tr/eng](http://www.ihbarweb.org.tr/eng)

[inhope@ihbarweb.org.tr](mailto:inhope@ihbarweb.org.tr)



A program of the Information and Communication Technologies Authority of the Republic of Turkey (ICTA), the Ihbar Web hotline was established as a report mechanism for potentially prohibited material found online. The ICTA is a regulatory authority of the Turkish government which oversees the Internet and Communications sectors, ensuring healthy industry competition and customer protection. In addition to regulatory responsibilities and hotline services, the ICTA offers outreach and Internet safety awareness programs and contributes to research and policy development for a safer Internet.

In 2007, the ICTA established the Ihbar Web hotline to respond to concerns of illegal material on the Internet. The hotline works closely with law enforcement, Internet Service Providers, policy makers and community organizations in pursuit of their mission. In addition to reports of possible child sexual exploitation, the hotline receives complaints concerning gambling, substance abuse, adult pornography, and self-harm material.

Reports are made to the hotline via telephone or online reporting form. Upon receipt of a complaint, the hotline assesses the nature of the reported content and then forwards to law enforcement reports containing apparently illegal material for further investigation.

Since its launch in 2007, the hotline has processed almost one million reports regarding potentially prohibited material, approximately 45,000 of which were concerning CSAM. In 2014 alone, the hotline received more than 9,000 reports regarding CSAM.

The hotline has strong relationships with both national and international organizations in its work to make the Internet a safer place for children. The Ihbar Web is part of the Turkish Safer Internet Centre and is an active member in the INHOPE global network of hotlines.



**IWF**  
**Internet**  
**Watch**  
**Foundation**

**STOP** Child Sexual  
Abuse Imagery Online

INTERNET WATCH FOUNDATION

United Kingdom  
[www.iwf.org.uk](http://www.iwf.org.uk)  
[feedback@iwf.org.uk](mailto:feedback@iwf.org.uk)

The Internet Watch Foundation® (IWF) is a non-profit organization established by the United Kingdom's Internet industry to ensure a safe online environment for users with particular focus on child sexual abuse material. In particular, the organization identifies four key components to its mission:

- Disrupt the availability of child sexual abuse content hosted anywhere in the world
- Protect children who are victims of sexual abuse from repeat victimization and public identification
- Prevent internet users from accidentally stumbling across child sexual abuse content
- Delete criminally obscene adult, and non-photographic child sexual abuse content hosted in the UK.

IWF partners closely with law enforcement, the Internet industry, families, communities, government, and other non-profits in their pursuit to eliminate child sexual abuse material and graphic adult pornography from the Internet.

Reports may be made to the hotline via email, telephone, postal delivery, online reporting form, or smartphone app. Upon receipt of a report a member of the hotline team reviews the content and attempts to locate where the material is hosted. If by a UK company, the hotline collaborates with law enforcement and the hosting company for investigation and removal of the illegal content. If hosted internationally, a report is referred via the INHOPE global network of hotlines to an organization in the country of the content. If content is outside of the INHOPE network, reports from the IWF are forwarded to INTERPOL, via the UK NCA (National Crime Agency) so they can be forwarded to the relevant Law Enforcement agencies in the appropriate country.

In addition to responding to reports of possible online CSAM, in 2014 the IWF began proactive services, giving their analysts the ability to actively search for criminal content and not just rely on inbound reports from external sources. As a result, the hotline can remove more content in a more time efficient way and IWF saw a 137% increase in actioned reports from the year prior.

Since its launch in 1996 the hotline has received over 500,000 reports of possible CSAM and in 2014 alone received 74,119 reports.

IWF is part of the UK's Safer Internet Centre and is a founding member of the global network of hotlines, INHOPE.

## CYBERTIPLINE

United States of America  
[www.missingkids.org/cybertipline](http://www.missingkids.org/cybertipline)  
 +1 800-843-5678



A program of the National Center for Missing & Exploited Children® (NCMEC), the CyberTipline® serves as the national reporting mechanism and clearinghouse for tips and leads about possible child sexual exploitation in the United States. NCMEC serves as the national clearinghouse and resource center for families, victims, private industry, law enforcement and the public to help find missing children, reduce child sexual exploitation and prevent child victimization. NCMEC receives federal grant and private foundation funding, corporate financial and in-kind donations, and private donations to maintain and enhance our 22 programs of work, including conducting community safety presentations, working with corporate and photo partners to disseminate thousands of posters of missing children each year, providing prevention resource materials and curricula to educators and schools, and engaging with parents, families, social service agencies, law enforcement, schools, government agencies and federal and state legislators on issues relating to missing and exploited children.

The CyberTipline has been in operation since 1998 and is one of the founding members of INHOPE. The CyberTipline receives reports via their online reporting form and telephone. Reports are triaged 24/7 and are submitted from a variety of sources, including the public, law enforcement, the Internet industry, and other INHOPE hotlines. The CyberTipline has eight reporting categories: Possession, Manufacture and Distribution of Child Pornography, Online Enticement of Children for Sexual Acts, Child Sex Trafficking, Sex Tourism Involving Children, Child Sexual Molestation, Unsolicited Material Sent to a child, Misleading Domain Names, and Misleading Words or Digital Images on the Internet. Although the CyberTipline does not advertise the acceptance of additional report types, NCMEC does receive some reports concerning cyberbullying, SPAM, adult pornography and suicide, among other report types.

Since the CyberTipline's inception in 1998, more than 6 million reports have been received and made available to law enforcement for independent review and potential investigation. In 2014 alone, the CyberTipline received over 1.1 million reports, of which over 1 million were identified by the reporter as related to CSAM. NCMEC makes CyberTipline reports available to more than 100 law enforcement agencies around the world through a Virtual Private Network (VPN) owned and operated by NCMEC. In countries where NCMEC does not have a VPN, Interpol's NCB Washington makes report information available to the appropriate agencies.



Copyright © 2015 National Center for Missing & Exploited Children®  
All rights reserved.

This project was supported by Google.org and Grant No. 2015-MC-FX-K001 awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.