

# INHOPE

## International Association of Internet Hotlines

### Lighthouse Case Study

---

**Online child sexual exploitation is global in scope and requires a global response. INHOPE coordinates** and promotes international efforts to protect children from online exploitation, as well as supporting member hotlines to do the same at the national and sub-national levels. It is an example of a robust and highly effective multi-stakeholder, international, technology-driven governance network.

INHOPE brings together actors from diverse sectors of society to govern issues and resolve challenges that are not being or cannot be adequately addressed by individual states.

# Table of Contents

Case in Brief	1
Internet-Facilitated Child Sexual Exploitation	1
Legislation and Regulations	3
Law Enforcement Capacity	3
Developing Policy Solutions	5
INHOPE	6
INHOPE's International Clearinghouse for Public Tips	8
Setting Standards for Internet Hotlines	10
Producing Knowledge about Online Sexual Exploitation	11
Designing Policy and Tools to Reduce Online Exploitation	12
Spearheading Innovative Multi-Stakeholder Solutions	13
Building a Global Multi-Stakeholder Governance Network	15
Implications for Network Leaders	16
Endnotes	20
About Global Solution Networks	23





## Case in Brief

INHOPE is an international association of Internet hotlines with the goal of eradicating online sexual exploitation of children. It maintains a network of 49 Internet hotlines in 43 countries for reporting illegal online content such as child pornography, luring children online and child prostitution. These hotlines have been central to establishing INHOPE as an international governance network as defined by the Global Solution Networks taxonomy.<sup>1</sup> Multi-stakeholder governance networks bring actors from diverse sectors in society together to govern issues or resolve challenges that are not being or cannot be adequately addressed by individual states.

INHOPE's governance network performs a series of important functions that are improving the ability of concerned stakeholders to address the problem of online sexual exploitation of children. Its member hotlines act as centralized coordination mechanisms for local and global action on reports from the public regarding suspected incidents of child sexual exploitation, which drastically reduces the burden on law enforcement and increases global capacity to combat this problem. It sets the standards by which online child sexual exploitation is discussed and addressed, establishing clear protocols and processes for international engagement on the issue. It also produces vital research and knowledge that provides the evidence for effective prevention strategies and policy responses. And, INHOPE and its member hotlines have leveraged their reputations as neutral and credible partners in the fight against online child sexual exploitation to bring together private sector actors, government departments, law enforcement agencies and other NGOs to establish multi-stakeholder collaborations such as the Canadian Coalition Against Internet Child Exploitation and the European Financial Coalition against Commercial Sexual Exploitation of Children Online.

The problem of online child sexual exploitation is global in scope and requires a global response. INHOPE coordinates and promotes international efforts to protect children from online exploitation, as well as supporting member hotlines to do the same at the national and sub-national levels.

## Internet-Facilitated Child Sexual Exploitation

The sexual exploitation of women and children is an ancient issue. The use of children for sex, however, is also one of the world's most universal and enduring prohibitions. As a result, virtually all societies have restrictions and punishments for those who engage in child prostitution, child trafficking, child sex tourism and child pornography. Psychiatric research has shown the effects of child sexual abuse to include depression, guilt, fear, sexual

dysfunction, regression, addiction and an inability to form healthy relationships.<sup>2</sup> Especially in cases where children are violated by family members or individuals they trust, the impact of child sexual abuse can be severe. Article 19 of the United Nations *Convention on the Rights of the Child* implores nation-states to “take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse.”<sup>3</sup> Yet, despite significant attention and resources being applied to the problem, child sexual exploitation persists today and children in all areas of the world are at risk.

The Internet is a powerful tool for groups with both positive and negative social goals and unfortunately sexual predators have long recognized that the same networked medium that gave rise to Wikipedia could also facilitate the exploitation of children. As early as 1995, law enforcement professionals and national governments were alerted to the fact that the Internet was being used to exchange images and promote child sexual exploitation.<sup>4</sup> What has become known as the “deep web”—that part of the Internet which is not indexed by major search engines and which is often password protected—is host to numerous criminal networks involved in drugs, weapons, murder and human trafficking.<sup>5</sup> In this space, the exchange of child pornography has been especially prolific, fueled by the creators, distributors and consumers of this “product.”



The part of the Internet which is publicly available and indexed by search engines is only a small fraction of the entire Internet. Far more Internet pages are only accessible by special access and are referred to as the “deep web.”<sup>6</sup>

Prior to the Internet, the child pornography industry was limited to mail-order catalogues and fairly isolated individuals, and was traced by law enforcement more easily than is now the case. The Internet allows the suppliers and consumers of child pornography to gather in online communities where their interest in sexually exploiting children is supported and facilitated.<sup>7</sup> The



Internet has also increased anonymity and protection from law enforcement for these individuals, and reduced the transaction cost of producing and exchanging child sexual abuse images to almost nothing. This dynamic has caused an explosion of child pornography online. It is estimated that the total number of child pornography images circulating online quadrupled between 2007 and 2011.<sup>8</sup> Estimates as to how much revenue the trade generates vary greatly, but a number in the billions of dollars each year is likely.<sup>9</sup> Furthermore, the demand for new images is exacerbating the issue of child sexual abuse offline because, in order to gain higher status within the online community, a consumer is often expected to contribute an image of their own creation.<sup>10</sup>

As the children portrayed in these images grow older, their victimization is compounded by the understanding that photos or videos of their abuse are being circulated amongst those who gain sexual gratification from their distress.<sup>11</sup> In the US, federal law mandates that child pornography victims be notified each time an offender is arrested and has a collection that includes an image depicting the victim. Certain images are distributed widely and so “it is not unusual for some victims to receive multiple official notifications each week.”<sup>12</sup> These notifications can be traumatic, reminding victims of how often the images of their abuse are viewed—but they are important if the victim wishes to seek restitution.

## Legislation and Regulations

Regulators at the international, regional and national levels have struggled to keep pace with the evolving sophistication of online child sexual exploitation. The United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, adopted in 2000, broadly defines child pornography as “any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.”<sup>13</sup> As adopted by the UN General Assembly, the protocol establishes this definition as the bare minimum upon which national policymakers should build. In practice, however, the definition of child pornography and the surrounding regulations vary significantly between regions and countries. This allows the perpetrators of these crimes to “forum shop” for geographies that offer the lowest risk for their activities. For example, the Canadian definition restricts child pornography including written exploitation (which the UK does not restrict) and accessing—or viewing—child pornography (which the US does not prohibit).

## Law Enforcement Capacity

Law enforcement agencies are widely empowered to find and prosecute individuals who participate in online child sexual exploitation. However, child pornography is borderless in nature. A picture taken in Ukraine can be hosted



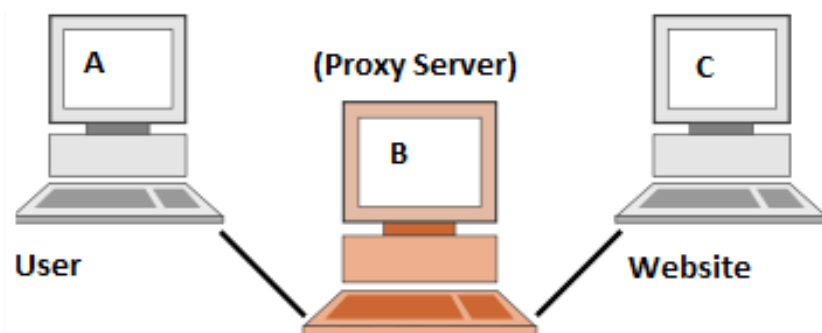
“Cybertip.ca watched one child exploitation website cycle through 212 unique IP addresses in 16 different countries over a 48-hour period.”

on a server in the US and accessed by someone in Canada. This leads to a conflict among law enforcement systems in different jurisdictions. According to Dr. Yaman Akdeniz, a leading academic<sup>14</sup> on the issue of cyber-rights and Internet governance:

*Criminal law is traditionally associated with nation-states and policing is a core activity of nation states. However, this legitimate activity is unsettled within a borderless medium such as the Internet. The policing of Internet child pornography is possible at a national level only when the perpetrators are within the jurisdiction of the nation-state, or when extra-territorial policing activity and cooperation is possible.<sup>15</sup>*

In some areas of the world, legislation regarding the sexual exploitation of children and associated enforcement mechanisms are strong. Europe, Canada and the US are among those who have invested significant resources in law enforcement capacity to target this problem. However, regions such as Eastern Europe and South Eastern Asia have limited regulation and resources, creating a vacuum in which child sexual exploitation flourishes.<sup>16</sup> The money to be made from illicit trade and tourism attracts those in impoverished and/or organized crime situations to take advantage of vulnerable populations.

Law enforcement agencies face severe knowledge deficits and resource constraints that undermine their capacity to deal with the problem of online child sexual exploitation. Those who use the Internet for illicit purposes are often technically savvy and utilize sophisticated techniques to hide their activities from police. For example, a 2009 research study by Cybertip.ca watched one child exploitation website cycle through 212 unique IP addresses in 16 different countries over a 48-hour period.<sup>17</sup> The use of proxy servers and zombie computers makes it very difficult for law enforcement to unravel the identities of those involved. Furthermore, the sheer scale of the problem means that police must dedicate significant resources to the triage, investigation and prosecution of child sexual exploitation incidents—resources that are typically scarce.



A proxy server functions as a relay between the user and a destination Web site. It hides the IP address of a user's computer from the Web site and may provide encryption. There are public access anonymous proxy servers on the Internet that can be used by anyone.

## Developing Policy Solutions

The explosion of child pornography has caused what some would call a “moral panic” in public opinion and pressure on governments to do more to combat the problem.<sup>18</sup> The apparent limitations of legislation and law enforcement have led to many recent initiatives to close loopholes, increase capacity and engage in public awareness and prevention activities. New legislation has been primarily focused on increasing the online monitoring capacity of law enforcement and making the punishments for crimes against children more severe. In Canada, for example, the Federal Government has enacted Bill C-22, *An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service*, which compels Internet Service Providers (ISPs) to report complaints from their subscribers of online child sexual exploitation to the Canadian Hotline Cybertip.ca and cooperate with law enforcement to investigate.<sup>19</sup> Recently, the Canadian Government has also passed legislation that imposes mandatory minimum sentences for sexual offenses against children and established the criminality of new forms of child sexual exploitation including: incidents where sexually explicit material is provided to a child during the process of grooming, and the use of information and communications technology to arrange for the sexual exploitation of a child. The addition of these crimes to the Canadian Criminal Code was largely based on research produced by Cybertip.ca that illuminated the particular ways in which child sexual exploitation was occurring online.<sup>20</sup>

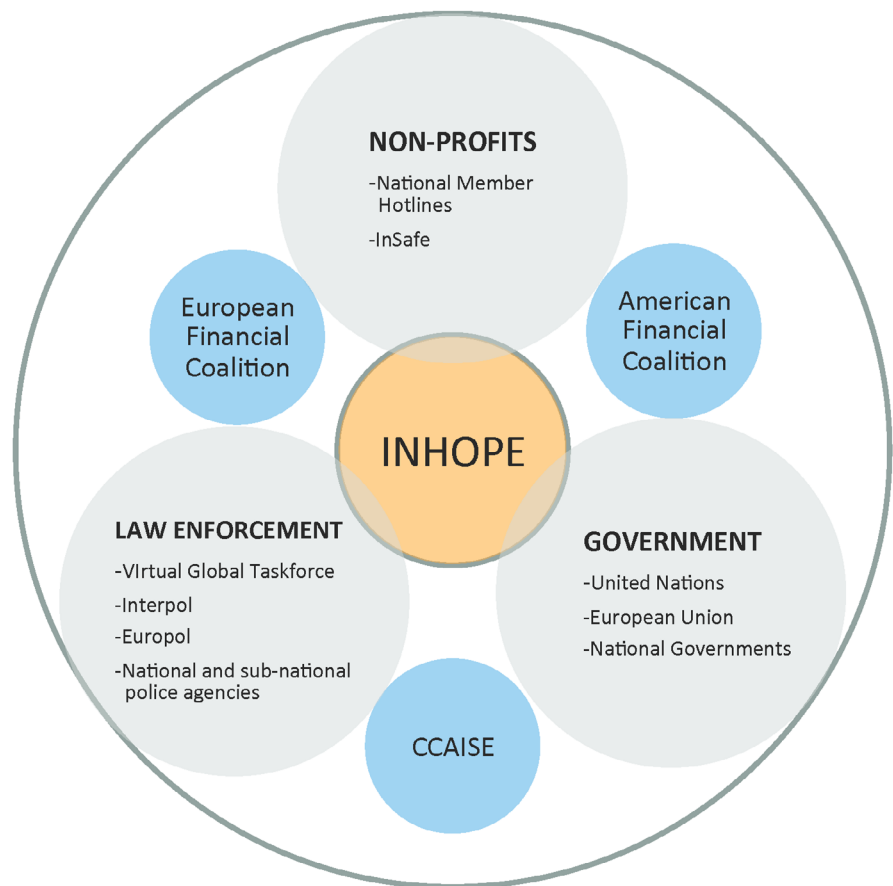
Despite the significant consensus that there is a need to combat online child sexual exploitation, these types of policy initiatives have also stirred up significant controversy.<sup>21</sup> Many groups—including those involved in the fight against Internet child exploitation—argue that the Internet should remain a free and open space and that individuals have an inalienable right to privacy, even online. Prominent academics such as Michael Geist, the Canada Research Chair in Internet and E-Commerce Law at the University of Ottawa, have repeatedly criticized the Canadian Federal Government for broadening the scope under which law enforcement agencies can request subscriber information from ISPs without a warrant—a request that was made over 1.1 million times in 2011.<sup>22</sup> Others argue that further criminalization and more jail time will push the problem deeper underground and do little to rehabilitate offenders.<sup>23</sup> In the face of these strong opinions, governments have had to walk a very fine line between increasing legislation and enforcement aimed at protecting children, while also respecting civil liberties.

In response to the enforcement gaps and evident controversy, INHOPE is seeking to convene a broader governance network to boost the capacity of law enforcement to combat online child sexual exploitation and bridge the divide among stakeholders over possible policy solutions. The network includes NGOs, private sector actors, governments, multilateral institutions and law enforcement agencies. A primary component of this system: non-profit “hotlines” that have been established at the national level to fill the resource gap of law enforcement agencies. These hotlines act as a clearing house for public complaints of child sexual exploitation, triaging them and conducting initial assessments that are then passed on to law enforcement.



However, as previously noted, a single incident of online child sexual exploitation can involve multiple jurisdictions around the world. At the center of this network is the INHOPE Association of Internet Hotlines—a global coordination center for the exchange of information related to online child sexual exploitation between hotlines and law enforcement agencies.

### Ecosystem of Organizations Combating Child Sexual Exploitation







## INHOPE

INHOPE and its member hotlines are playing a number of vital roles in exposing the problem of online child sexual exploitation and spearheading innovative solutions. It sets international standards and protocols for discussing and addressing online child sexual exploitation. It produces knowledge about how online exploitation practices are evolving and advises policy makers on how to respond. It runs powerful public awareness campaigns and seeks to empower ordinary citizens to participate in protecting children by reporting suspected online child sexual exploitation. It also maintains a centralized clearinghouse between the public and law enforcement agencies that ensures that tips from the public are validated and then routed to the appropriate law enforcement officials in countries around the world. In performing all of these services, INHOPE and its members have established an effective governance network that supplements global capacity to address this problem. As frontline service providers, hotlines deliver the added manpower and expertise necessary for law enforcement and child protection agencies to focus their resources on apprehending the perpetrators of these crimes and rescuing their victims. They are also in a unique arms-length position from government and law enforcement that mitigates concerns about state surveillance.

Importantly, INHOPE has been able to shed light and open public discussion on an otherwise opaque and sensitive topic through research, and the study of child sexual abuse images. Characteristics of child pornography victims and offenders have often been misconstrued and limited to stereotypes (pedophiles are strange looking and the victims are willing adolescents) due to a lack of research on the issue. In fact, as the statistics previously cited show, the children are often very young and subjected to severe sexual assaults; the offenders are often known and well regarded individuals in the child's life. INHOPE improves law enforcement techniques and creates more effective public awareness materials that help adults to better understand the risk factors of child sexual abuse, to recognize its symptoms in children, and to implement prevention and intervention strategies.

INHOPE has also been at the forefront of innovative multi-stakeholder solutions and fostered collaboration between industry competitors. Specifically, national hotlines have been instrumental in bringing together different ISPs on collaborative projects that otherwise would have been focused on carving out niche corporate responsibility roles aimed at garnering more loyalty from their customers. For example, Bell Canada focuses on providing support for mental health initiatives while TELUS raises money for environmental causes—yet they work together alongside the other major Canadian ISPs with Cybertip.ca on the Canadian Coalition Against Internet Child Exploitation.

INHOPE and its member hotlines have fostered a dynamic and effective global governance network that has dramatically improved the capacity of relevant stakeholders to combat online child sexual exploitation. For example, since 2002, Canada's national hotline Cybertip.ca has received



over 94,000 reports from the public. 22,000 of those reports have been forwarded to law enforcement (23%) and 15,000 were forwarded to INHOPE for international action (15%).<sup>24</sup> Those reports deemed to have actionable information for Canadian law enforcement have resulted directly in more than 125 arrests and over 62 children being removed from abusive environments.<sup>25</sup> In 2012, Canadian Public Safety Minister Vic Towe described Cybertip.ca as a “critical partner” and stated:

*[Cybertip.ca has] the knowledge and expertise to provide insight into the multi-faceted world of cybercrime. Specifically, Cybertip.ca provides services that support Canada’s law enforcement agencies in the fight against individuals who use the Internet to target children.<sup>26</sup>*

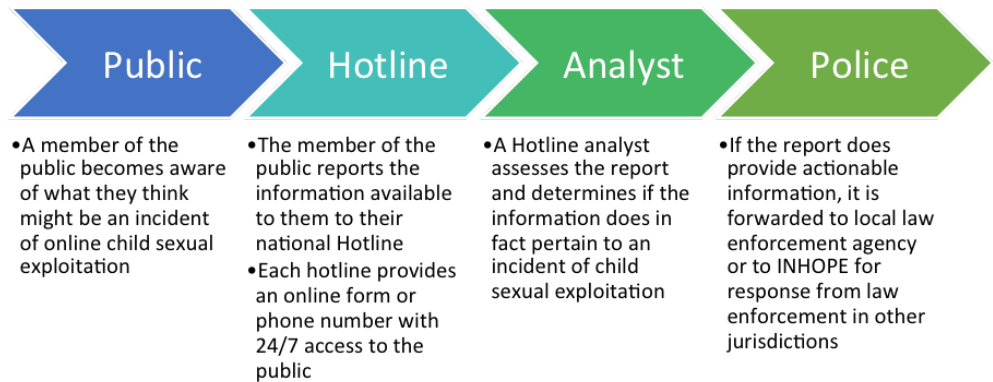
Internationally it is estimated that this network has contributed to the arrests of thousands of offenders and the greater protection of countless children.

## INHOPE’s International Clearinghouse for Public Tips

Almost as quickly as it became clear that the Internet was facilitating a drastic increase in child sexual exploitation, it became apparent that alternative methods would be needed to augment the capabilities of law enforcement and governments to combat the surge. In 1995, an organization called Childnet International<sup>27</sup> was established in the UK with the aim to “showcase the positive, transforming ways in which the new technologies could help young people as well as helping them to stay safe online.”<sup>28</sup> The first Internet hotline was established in Holland in June of 1996.<sup>29</sup> This was quickly followed by hotlines throughout Europe and shortly thereafter, the concept expanded to North America, Asia and Australia, South Africa and South America.<sup>30</sup> All hotlines are non-profits and the majority are non-governmental organizations. Some are run by larger organizations dedicated to children’s issues such as the Canadian Centre for Child Protection<sup>31</sup> or the National Center for Missing and Exploited Children<sup>32</sup> in the US.

The hotlines act as a central place to accept and triage tips from the public regarding online child sexual exploitation, particularly child pornography. Tips are scrutinized against a hotline’s national standard of child pornography and if the complaint does in fact pertain to a verified incident of online child sexual exploitation, the details are forwarded to law enforcement.



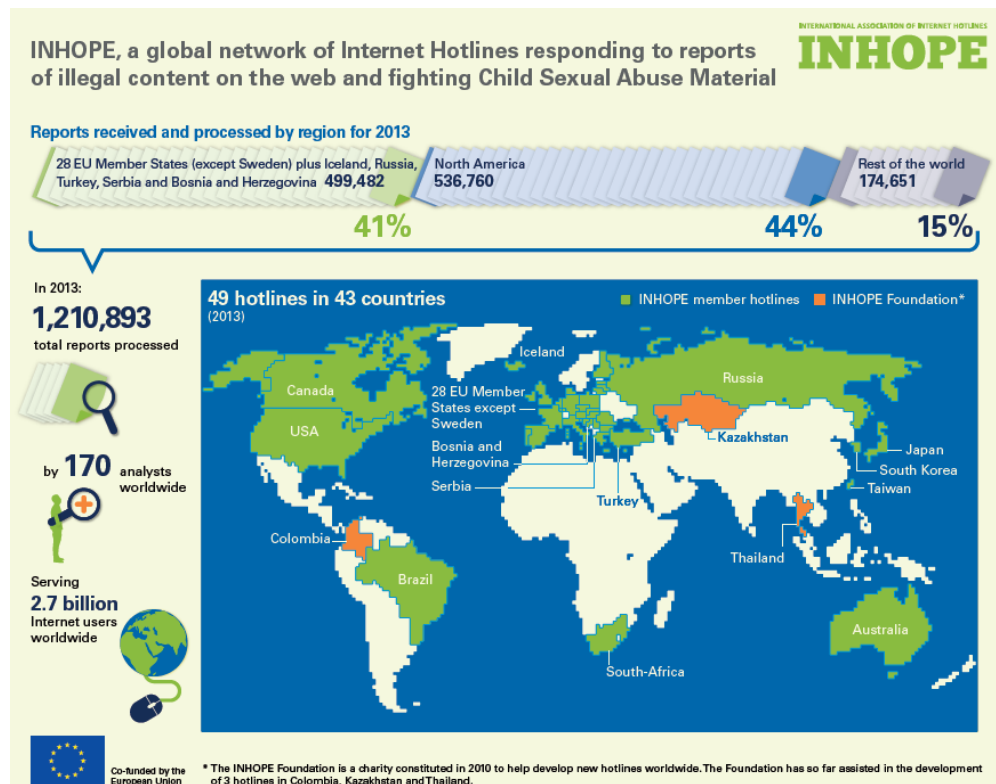


The INHOPE public reporting triage process

In cases where it is determined that a complaint is legitimate, but the information relates to individuals or websites outside of the local jurisdiction, the information must be forwarded internationally. This results in a vast and complex web of relationships between the various hotlines and the seemingly infinite municipal, provincial, national, regional and international law enforcement entities. By 1997, it was clear that better coordination and cooperation were needed between the various groups. Childnet secured funding from the European Commission's Daphne Programme<sup>33</sup> which offers grants to private or public organizations that work to prevent and combat violence against children, young people and women.<sup>34</sup> With this funding, Childnet organized the first INHOPE Forum in 1999, from which 8 hotlines incorporated the INHOPE Association of Hotlines. Headquartered in Holland, INHOPE has since grown to include 49 hotlines in 43 countries (see Appendix).<sup>35</sup>

INHOPE acts as an international clearinghouse for the exchange of information related to online child sexual abuse between hotlines and law enforcement agencies. When a national hotline determines that an incident of exploitation is outside of its own law enforcement's jurisdiction, the information is uploaded to INHOPE's "resource management database." The information is then downloaded by the relevant national hotline and the tip is processed for its own local law enforcement.<sup>36</sup> This process establishes a clear chain of communication between hotlines and law enforcement and results in a more efficient and effective global response to online child sexual exploitation.





Map of hotlines in the INHOPE network<sup>14</sup>

## Setting Standards for Internet Hotlines

INHOPE has worked diligently to build its reputation and is well respected by law enforcement agencies as a valuable partner. In order to belong to INHOPE, member hotlines must abide by a Code of Practice which details the minimum standards required. These include: the provision of a public reporting mechanism for online child sexual exploitation; access to safety and prevention materials; data protection protocols; identity protection for both public reporters and hotline staff; best practices on report exchange; and internal policies and procedures for staff welfare and tip processing, as well as transparency on what information is provided to law enforcement.<sup>38</sup>

In recognition that establishing an effective hotline requires significant resources, the INHOPE Foundation was created in 2010. The Foundation provides financial support and expertise to start-up hotlines in countries considered to be primary sources of online child sexual exploitation. Currently, the INHOPE Foundation is supporting the development of hotlines in Columbia, Kazakhstan and Thailand. INHOPE also works to achieve policy alignment across nation states on the definitions of and responses to the various types of online child sexual exploitation, increasing global coordination and eliminating areas where child exploitation thrives.

“In 2013, INHOPE members processed over 1.2 million reports from the public on suspected incidents of online child sexual exploitation. Of those reports that were uploaded to INHOPE and pertained to child pornography, 71% depicted the abuse of pre-pubescent children and 10% pertained to infants.”

## Producing Knowledge about Online Sexual Exploitation

INHOPE and its member hotlines are in a unique position to produce statistics and research on the issue of online child sexual exploitation—shedding light on an otherwise rarely examined and often misunderstood social issue. Understanding the scope and nature of the problem is vital to ensuring that policy and law enforcement responses are effective. Furthermore, hotlines are able to identify emerging trends and can act as an early warning system for new types of child exploitation.

There are those who argue that “child pornography” primarily consists of harmless photos of nude children or that it depicts the consensual activity of teenagers. Statistics are vital to counteracting these perceptions. In 2013, INHOPE members processed over 1.2 million reports from the public on suspected incidents of online child sexual exploitation.<sup>39</sup> Of those reports that were uploaded to INHOPE and pertained to child pornography, 71% depicted the abuse of pre-pubescent children and 10% pertained to infants. Girls are represented in over 80% of the images and are typically Caucasian.<sup>40</sup> An extensive research report by Cybertip.ca in 2009 also found that the majority of images processed depicted children under the age of 12 and that in 37.2% of those images, the children are being subjected to sexual assault.<sup>41</sup> Most alarmingly, the report found that the most extreme acts of sexual abuse typically involved children under the age of 8. The report also determined that the top five countries for hosting websites of child sexual abuse images are the US, Russia, Canada, Japan and South Korea.<sup>42</sup> These statistics show child pornography for what it is—reproduced images of child sexual abuse.

INHOPE and member hotlines produce powerful public awareness campaigns aimed at both improving the understanding of child sexual abuse and empowering protective adults to take action by reporting abuse and implementing prevention strategies. The Cybertip.ca report declared that while hotlines and law enforcement were doing significantly better at curbing the demand for child pornography, more needed to be done to eradicate the supply of images in the first place:

*The truth is that sexual abuse begins in the offline world. Efforts should be focused on preventing child sexual abuse from occurring in homes and communities. By doing so, we reduce the likelihood of these images circulating on the Internet.*<sup>43</sup>

The research and statistics produced by INHOPE and its member hotlines reveal the characteristics of victims, offenders and the countries affected—no area or demographic is immune. This information has been translated into better education and public awareness materials for children, adults, educators, social services and law enforcement. INHOPE works in partnership with InSafe<sup>44</sup> to promote prevention and public awareness materials internationally. Every year since 2004, InSafe has coordinated Safer Internet Day, which is now celebrated in over 100 countries.<sup>45</sup> The event empowers



member hotlines to distribute cutting-edge educational information and engage youth and adults in public discussion on the safe and respectful use of the Internet. In Canada, Cybertip.ca distributed over 1.3 million pieces of educational material to over 7,000 schools on Safer Internet Day 2014.<sup>46</sup>



INHOPE's Safer Internet Day is now celebrated in more than 100 countries and is used by member hotlines to distribute online safety materials to children and adults, as well as to engage in public conversation on issues of Internet safety such as cyber bullying, self/peer exploitation and luring.<sup>47</sup>

## Designing Policy and Tools to Reduce Online Exploitation

INHOPE and its member hotlines are the first to become aware of emerging types of online child sexual exploitation and are more agile than other stakeholders to begin producing prevention and intervention tools. For example, in recent years, two primary issues have emerged: luring and self/peer exploitation. Luring involves the systematic grooming of vulnerable children by Internet predators who convince those children to share sexualized images or arrange to meet them in person for sexual contact. Self/peer exploitation refers to what might otherwise be called “sexting” except that the images end up online.

Hotlines have been reporting increasing incidents of these types of exploitation, have been contacted directly by distraught children and parents, and are acutely aware of cases where children have chosen to take their own lives as a result of this type of targeting. Hotlines are in the unique position to understand how these types of exploitation occur and have worked to craft specific education and prevention materials for these

issues.<sup>48</sup> As previously discussed, they have also worked with policy makers and Internet companies to create new legislation to include these offenses in criminal codes and have pressed industry partners to develop mechanisms for more effective content removal. Childnet International sits on Facebook's Safety Advisory Board, for example, and assists in developing mechanisms and materials to address issues such as cyberbullying, requesting the removal of photos, and "think before you post" public awareness campaigns.<sup>49</sup>

## Spearheading Innovative Multi-Stakeholder Solutions

INHOPE and its member hotlines have played a vital role in spearheading innovative multi-stakeholder governance solutions to the problem of online child sexual exploitation. As non-profits and non-governmental organizations, hotlines offer a neutral legitimacy that can bring competitive or dissimilar actors together to tackle thorny issues. Essential to the recent acceleration of online child sexual exploitation are those service providers and companies whose products provide the space and tools used by online offenders. However, convincing private sector actors of their culpability, and their social responsibility to participate in the fight against Internet child sexual exploitation—let alone expecting them to take on the added costs of building in prevention mechanisms that make it more difficult for their services to be used by child sex offenders—continues to be challenging.

As previously discussed, Canadian ISPs support Cybertip.ca financially and participate collaboratively in CCAISE. In the US and Europe, credit card companies—including both Visa and MasterCard—work together on financial coalitions aimed at preventing the use of these payment services in the commercial sexual exploitation of children. Furthermore, where tensions have existed between these private sector entities and the desire of law enforcement or government actors to tighten regulations or mandate information sharing, member hotlines have used these coalitions as a space to foster confidence building and voluntary solutions.

Research from INHOPE and its network reveals that when it comes to commercial child pornography—that is, child pornography that requires payment before access—both online payment systems and major credit cards are being used for the transactions. In response, INHOPE and its members have been instrumental in establishing private-public partnerships and industry cooperation to make significant progress towards eradicating the misuse of financial services. In 2006, the National Center for Missing & Exploited Children (an American hotline), established the Financial Coalition against Child Pornography. The coalition includes "34 leading banks, credit card companies, electronic payment networks, third-party payments companies and Internet service companies dedicated to putting an end to commercial child pornography."<sup>50</sup> Members include Visa, MasterCard, Microsoft, Bank of America, GoDaddy.com and Western Union. Similarly in Europe, INHOPE spearheads the *European Financial Coalition against*





*Commercial Sexual Exploitation of Children Online* alongside Europol, Google, MasterCard, PayPal, Microsoft and Visa.



Member hotlines such as Cybertip.ca conduct public awareness campaigns to encourage the public to report online child sexual exploitation. The multi-stakeholder nature of these efforts is exemplified here by the addition of public and private sector logos that represent support of Cybertip.ca and contribute to positive public relations and corporate social responsibility for these organizations.<sup>51</sup>

These coalitions work to establish best practices for the financial industry in preventing and detecting the use of their services for the commercial sexual exploitation of children. Some companies have become industry leaders on the issue and have built their efforts into their brand. PayPal, for example, has developed proprietary models designed to detect the use of their services for child exploitation, employs over 100 agents globally to investigate violations, and works directly with law enforcement to identify offenders.<sup>52</sup>

A number of obvious solutions to the problem of child pornography—solutions within the power of Internet service providers and infrastructure providers to advance—are the ideas of blocking access to certain websites, shutting down servers that are hosting illegal content, and connecting subscriber information with the anonymous IP addresses that hotlines and law enforcement observe engaging in online child sexual exploitation. In Canada, Cybertip.ca initiated CCAISE, which includes federal government departments, law enforcement agencies, related NGOs and representatives from the major ISPs.<sup>53</sup> The Coalition has worked to build confidence and cooperation between members, particularly between ISPs and law enforcement agencies. This initiative has since created the Cleanfeed Canada system—a list managed by Cybertip.ca of foreign websites that host child pornography. ISPs use the list (voluntarily) to block their customers' access to websites determined to host child sexual abuse content.

Since being established in 2006,<sup>54</sup> Cybertip.ca has added over 17,500 URLs to the system and all major Canadian ISPs participate. CCAISE has also





facilitated a systematic process for the request of customer information from law enforcement to ISPs, as well as notice-and-takedown processes. These methods have been controversial; German legislators, for instance, were forced to abandon a proposal to implement a police-run Internet filtering system in the face of public backlash against censorship.<sup>55</sup> However, in countries where hotlines have been designated as the managers of these systems, at arms-length from government and law enforcement, they have been more publicly acceptable and successful as a result.

## Building a Global Multi-Stakeholder Governance Network

The Internet has facilitated an explosion of online child pornography and it continues to flourish in legislative and law enforcement vacuum. Although the problem of online child sexual exploitation is inherently international, jurisdictional boundaries have limited the effectiveness of law enforcement agencies to enforce national and international child protection laws. Limited resources and the slow pace of policy development mean that governments struggle to deal with the problem. Limited public awareness and prevention strategies have hindered the ability to protect children from those who seek to exploit children online. Child sexual abuse and child pornography have been discussed rarely, and are often misunderstood in the public sphere. These factors have contributed to an exponential increase in child sexual exploitation on and offline.

In response to each of these limitations, INHOPE has built a networked solution that brings in multiple stakeholders from across geographical and industry lines to effect change. It provides the public with centralized portals to report suspected incidents of online child sexual exploitation. Hotline analysts triage and scrutinize the reports, passing only actionable information on to law enforcement—greatly reducing the workload and resources required by these agencies to manage the problem. INHOPE's standard setting initiatives ensure that information is exchanged in a reliable and efficient manner and provides consistent protocols for managing reports of online child sexual abuse across all jurisdictions in the network. Its research and data analysis produces new knowledge about the problem and timely information on emerging trends. This knowledge ensures evidence-based policy solutions and effective prevention and education materials for law enforcement and the general public. Where solutions require other stakeholders to become involved, INHOPE and member hotlines have facilitated the necessary connections and trust to develop multi-stakeholder solutions.

In its totality, INHOPE, member hotlines, and the surrounding ecosystem of law enforcement, government, and private sector actors, have established a sophisticated and effective global governance network against the issue of online child sexual exploitation. INHOPE and its members have been central to this network's development—pushing the relevant stakeholders to better



understand the problem, apply the necessary resources more effectively, and cooperate with each other to overcome major obstacles. They have offered a neutral space for the development of innovative solutions that mitigate concerns about privacy violations and censorship. They have achieved significant success. INHOPE reports that in 2013, over 93% of online child sexual exploitation material is removed within one week thanks to notice-and-takedown procedures, up from 82% in 2011.<sup>56</sup> 2013 also saw the arrest of Eric Eoin Marques—widely considered to be the largest facilitator of child pornography in the world—and shut down his hosting website, on which many of the world’s largest child pornography websites relied.<sup>57</sup> For its role in this operation, INHOPE offers valuable insights for network leaders operating in other areas of law enforcement and Internet governance.

## Implications for Network Leaders

**Governance networks can significantly augment the capacity of traditional law enforcement to combat illicit trade online.** Trafficking—whether in weapons, drugs or humans—is an entrenched global problem that flourishes in areas where existing laws and enforcement capabilities are weak. Due to resource constraints and limited expertise, regulatory and law enforcement capacity are especially weak when it comes to combating these problems online.

**The global multi-stakeholder network centered on INHOPE demonstrates that the most difficult of problems can be addressed effectively through a decentralized and cooperative approach.** Law enforcement agencies have been reluctant to allow other actors to become involved in crime fighting due to the obvious and justified fear of vigilantism. However, through the legitimacy derived from government support and demonstrated value-add, INHOPE and its members have negotiated a vital role in coordinating and facilitating global cooperation against the seemingly intractable problem of online child sexual exploitation. They have reduced the burden on law enforcement agencies, garnered the participation of relevant private sector stakeholders, and empowered the public to assist and take preventative actions. These elements could not have been achieved by any one actor alone.

**Governance networks can provide the necessary neutral and trusted space for compromise in Internet governance.** The primary obstacles to preventing crime and exploitation online are important concerns about the slippery slope of state surveillance and censorship. In light of recent revelations, such as the sweeping surveillance program operated by the United States National Security Agency, the public is increasingly skeptical of further legislative proposals to monitor the Internet—even in the name of child protection. NGO-led networks offer an alternative to state controlled



policy and enforcement mechanisms. By operating at arms-length from both government and law-enforcement, INHOPE and its member hotlines provide a trustworthy service to the public and ensure that law enforcement resources are focused on verified incidents of child sexual exploitation.

**Governance network leaders can use a range of tactics to bring the necessary stakeholders together.** It is within their capability to name and shame governments and private sector actors who do not participate in the fight against online child sexual exploitation. However, it is also within their capability to support the public relations campaigns and corporate social responsibility initiatives of those stakeholders that do engage on the issue. Networks can also facilitate behind-the-scenes negotiations before bringing the necessary stakeholders to the table so that collaboration can take place quickly and effectively. The INHOPE network and its member hotlines have been incredibly effective at identifying the role each relevant stakeholder plays in perpetuating the problem of online child sexual exploitation and outlining what each organization has to gain by participating in the creation of targeted solutions.

**Governance networks can desensitize and illuminate issues that societies struggle to understand and mitigate.** Child sexual abuse and child pornography have been some of the most difficult subjects for public discussion due to the secrecy necessary for the offense and the sense of guilt and shame often felt by the victims. The INHOPE network has worked to open the public discussion by presenting extensive research and statistics that clarify and desensitize the subject matter. This has allowed policy makers to make evidence-based decisions on how to address the problem and enabled law enforcement to focus their efforts where they have the most impact. Networks working in other areas such as climate change or mental illness can play an invaluable role in multiple areas of ensuring accurate understandings and effective response mechanisms.

*By Mary Milner for Global Solution Networks*



## Appendix— INHOPE Member Hotlines

Australia	Australian Communications and Media Authority
Austria	Stopline
Belgium	StopChildPorno.be
Bosnia and Herzegovina	Sigurno Dijete
Brazil	SaferNet Brasil
Bulgaria	Safer Internet Hotline
Canada	Cybertip.ca
Columbia	Te Protejo
Croatia	Center for Missing and Exploited Children
Cyprus	Safer Internet Hotline
Czech Republic	Horkalinka.cz
Denmark	Save the Children Denmark
Estonia	Vihjeliin
Finland	Save the Children Finland
France	PointeDeContact.net
Germany	<ul style="list-style-type: none"> <li>• Internet-beschwerdestelle.de</li> <li>• Voluntary Self-Monitoring of Multimedia Service Providers</li> <li>• Jugendschutz.net</li> </ul>
Greece	SafeLine.gr
Hungary	biztonsagosinternt.hu Internet Hotline
Iceland	Save the Children Iceland
Ireland	Hotline.ie
Italy	Telefono Azzurro Save the Children Italy, Stop-It.org
Japan	Internet Hotline Center Japan
Kazakhstan	Internet Association of Kazakhstan
Korea	Korean Communications Standards Commission
Latvia	DrossInternets.lv
Lithuania	Draugiskas Internetas
Luxembourg	Bee Secure Stopline
Malta	Child Web Alert
Netherlands	Muldpunt Kinderporno op Internet
Poland	Dyzurnet.pl
Portugal	Linha Alerta Internet Segura



Romania	<a href="http://Safernet.ro">Safernet.ro</a>
Russia	<a href="#">Russian Safer Internet Centre</a> <a href="#">Friendly Runet Foundation</a>
Serbia	<a href="#">Net Parola</a>
Slovakia	<a href="http://Stopline.sk">Stopline.sk</a>
Slovenia	<a href="#">Spletno Oko</a>
South Africa	<a href="#">Film and Publication Board Pro Child Internet Hotline</a>
Spain	<ul style="list-style-type: none"><li>• <a href="#">Alia2 Foundation</a></li><li>• <a href="http://Protegeles.com">Protegeles.com</a></li></ul>
Taiwan	<a href="#">Web547</a>
Thailand	<a href="http://Thaihotline.org">Thaihotline.org</a>
Turkey	<a href="#">Telecommunications Presidency Internet Hotline, ihbarweb.org</a>
United Kingdom	<a href="#">Internet Watch Foundation</a>
United States	<a href="#">Cybertipline</a>



## Endnotes

- <sup>1</sup> Don Tapscott, “Introducing: Global Solution Networks,” Global Solution Networks, 2013. <http://gsnetworks.org/introducing-global-solution-networks/>
- <sup>2</sup> “Understanding Child Sexual Abuse: Education, Prevention and Recovery,” American Psychological Association. <http://www.apa.org/pubs/info/brochures/sex-abuse.aspx#>
- <sup>3</sup> United Nations, Office of the High Commissioner for Human Rights, “Article 19” Convention on the Rights of the Child, 20 November 1989. <http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>
- <sup>4</sup> “Our History,” INHOPE. <http://www.inhope.org/gns/who-we-are/Ourhistory.aspx>
- <sup>5</sup> Andrea Janus, “Diving into the Deep Web: What is it and can you access it?” CTV News 12 May 2014. <http://www.ctvnews.ca/sci-tech/diving-into-the-deep-web-what-is-it-and-can-you-access-it-1.1817334>
- <sup>6</sup> [http://www.chip.de/artikel/Darknet-Das-Tor-ins-Deep-Web-4\\_63227270.html](http://www.chip.de/artikel/Darknet-Das-Tor-ins-Deep-Web-4_63227270.html)
- <sup>7</sup> U.S. Department of Justice, “The National Strategy for Child Exploitation Prevention and Interdiction: A Report to Congress,” August 2010. <http://www.justice.gov/psc/docs/natstrategyreport.pdf>, p 3.
- <sup>8</sup> <http://www.sumall.org/child-pornography-data/>
- <sup>9</sup> Supra note 7, p 15.
- <sup>10</sup> Supra note 7, p 18.
- <sup>11</sup> Supra note 7, p 9.
- <sup>12</sup> United States Sentencing Commission, “Report to the Congress: Federal Child Pornography Offenses,” December 2012. <http://www.ussc.gov/news/congressional-testimony-and-reports/sex-offense-topics/report-congress-federal-child-pornography-offenses>, p 319.
- <sup>13</sup> United Nations, General Assembly, “Article 2,” Optional protocols to the Convention on the Rights of the Child on the involvement of children in armed conflict and on the sale of children, child prostitution and child pornography, 25 May 2000. <http://www.un-documents.net/a54r263.htm>
- <sup>14</sup> Dr. Yaman Akdeniz, “About,” CyberLaw Blog. <http://cyberlaw.org.uk/about/>
- <sup>15</sup> Dr. Yaman Akdeniz, Internet Child Pornography and the Law: National and International Responses, May 2008, p 2.
- <sup>16</sup> “Combating Child Sex Tourism: Questions & Answers,” ECPAT International, 2008. [http://www.ecpat.net/sites/default/files/cst\\_faq\\_eng.pdf](http://www.ecpat.net/sites/default/files/cst_faq_eng.pdf), p 7.



- <sup>17</sup> “Child Sexual Abuse Images: An Analysis of Websites by Cybertip.ca,” Cybertip.ca, 2009. [https://www.cybertip.ca/pdfs/CTIP\\_ChildSexualAbuse\\_Report\\_en.pdf](https://www.cybertip.ca/pdfs/CTIP_ChildSexualAbuse_Report_en.pdf), p 11.
- <sup>18</sup> Supra note 15, p 15.
- <sup>19</sup> “Mandatory Reporting,” Cybertip.ca. [https://www.cybertip.ca/app/en/projects-mandatory\\_reporting](https://www.cybertip.ca/app/en/projects-mandatory_reporting)
- <sup>20</sup> “Preliminary Findings Provide New Insight Into the Crime of Online Luring,” Cybertip.ca, 19 October 2012. [https://www.cybertip.ca/app/en/media\\_release\\_online\\_luring](https://www.cybertip.ca/app/en/media_release_online_luring)
- <sup>21</sup> Supra note 15, p 2.
- <sup>22</sup> Michael Geist, “Five Measures to Help Counter the Tidal Wave of Secret Telecom Disclosures,” michaelgeist.ca, 6 May 2014. <http://www.michaelgeist.ca/content/view/7121/135/>
- <sup>23</sup> Parliamentary Task Group on the Sexual Abuse of Children, “Report of the Parliamentary Task Group on the Sexual Abuse of Children,” Government of New Zealand, 2002. [www.govt.nz/documents/download.php?f=70225](http://www.govt.nz/documents/download.php?f=70225), p 67.
- <sup>24</sup> “Our Results: Reporting and Education,” Cybertip.ca. [https://www.cybertip.ca/app/en/about#about-our\\_results](https://www.cybertip.ca/app/en/about#about-our_results)
- <sup>25</sup> Ibid.
- <sup>26</sup> “Cybertip.ca: A 10 Year Review of Canada’s Tipline for Reporting the Online Sexual Exploitation of Children,” Cybertip.ca, 2012. [https://www.cybertip.ca/pdfs/CTIP\\_10YearReport\\_en.pdf](https://www.cybertip.ca/pdfs/CTIP_10YearReport_en.pdf), p 7.
- <sup>27</sup> “Home,” Childnet International. <http://www.childnet.com/>
- <sup>28</sup> “Where did it all begin,” Childnet International. <http://www.childnet.com/what-we-do/where-did-it-all-begin>
- <sup>29</sup> “Home,” Meldpunt Kinderporno op internet. <http://www.meldpunt-kinderporno.nl/en/>
- <sup>30</sup> “At A Glance,” INHOPE.org. <http://www.inhope.org/gns/who-we-are/at-a-glance.aspx>
- <sup>31</sup> “Home,” Canadian Centre for Child Protection. <https://www.protectchildren.ca/app/en/>
- <sup>32</sup> “Home,” National Center for Missing & Exploited Children. <http://www.missingkids.com>
- <sup>33</sup> “Daphne III,” European Commission. <http://ec.europa.eu/justice/fundamental-rights/programme/daphne-programme/>
- <sup>34</sup> Ibid.
- <sup>35</sup> Supra note 30.
- <sup>36</sup> “INSAFE – INHOPE working together for a better Internet for children and young people: Annual Report 2013,” INHOPE, April 2014. <http://www.inhope.org/tns/resources/annual-reports.aspx>, p 9.



- <sup>37</sup> <http://inhope.org/tns/resources/statistics-and-infographics.aspx> April 27 2014
- <sup>38</sup> “Code of Practice,” INHOPE, 2013. [http://inhope.org/Libraries/Best\\_Practice\\_Papers/2013\\_Code\\_of\\_Practice\\_update.sflb.ashx](http://inhope.org/Libraries/Best_Practice_Papers/2013_Code_of_Practice_update.sflb.ashx)
- <sup>39</sup> “2013 Infographics,” INHOPE, April 2014. <http://www.inhope.org/Libraries/Infographics/INHOPE-2013-Inforgraphic.sflb.ashx>, p 1.
- <sup>40</sup> Ibid, p 3.
- <sup>41</sup> Supra note 17, p 2.
- <sup>42</sup> Ibid, p 4.
- <sup>43</sup> Ibid, p 5.
- <sup>44</sup> “Home,” InSafe. <http://www.saferinternet.org/>
- <sup>45</sup> “About Safer Internet Day,” InSafe. <http://www.saferinternetday.org/web/guest/about>
- <sup>46</sup> News and Media, “Safer Internet Day,” Canadian Centre for Child Protection. [https://www.protectchildren.ca/app/en/news\\_releases#news\\_releases-safer\\_internet\\_day](https://www.protectchildren.ca/app/en/news_releases#news_releases-safer_internet_day)
- <sup>47</sup> <http://www.saferinternetday.org/web/guest/home>
- <sup>48</sup> “Home,” NeedHelpNow.ca. <http://www.needhelpnow.ca/app/en/>
- <sup>49</sup> “Family Safety Centre,” Facebook.com. <https://www.facebook.com/safety>
- <sup>50</sup> “Financial Coalition Against Child Pornography,” National Center for Missing & Exploited Children. <http://www.missingkids.com/FCACP>
- <sup>51</sup> [https://www.cybertip.ca/images/content/projects-public\\_awareness/candy-en.jpg?r=20140418](https://www.cybertip.ca/images/content/projects-public_awareness/candy-en.jpg?r=20140418)
- <sup>52</sup> Financial Coalition Against Child Pornography, “Technology Challenges Working Group Report 2008: Trends in Migration, Hosting and Payment for Commercial Child Pornography Websites,” National Center for Missing & Exploited Children, 2008. [http://www.missingkids.com/en\\_US/documents/FCACP\\_Technology\\_Challenges.pdf](http://www.missingkids.com/en_US/documents/FCACP_Technology_Challenges.pdf)
- <sup>53</sup> “CCAICE,” Cybertip.ca. <https://www.cybertip.ca/app/en/projects-ccaice>
- <sup>54</sup> “Mountie hopes web initiative could cut child abuse,” CBC News, 23 November 2006. <http://www.cbc.ca/news/technology/mountie-hopes-web-initiative-could-cut-child-abuse-1.592081>
- <sup>55</sup> T. J. McIntyre, “Child Abuse images and Cleanfeeds: Assessing Internet Blocking Systems,” School of Law University College Dublin, 23 July 2011. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1893667](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1893667), p 1.
- <sup>56</sup> Supra note 38.
- <sup>57</sup> Patrick Howell O’Neill, “An in-depth guide to Freedom Hosting, the engine of the Dark Net,” *The Daily Dot*, 4 August 2013. <http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/>





## About Global Solution Networks

Global Solution Networks is a landmark study of the potential of global web-based and mobile networks for cooperation, problem solving and governance. This research project is a deliverable of the GSN program, offered through the Martin Prosperity Institute at the Rotman School of Management, University of Toronto.

## Program Management

Don Tapscott, Executive Director  
Dr. Joan Bigham, Managing Director  
Anthony Williams, Executive Editor

## GSN Program Membership

Membership in Global Solution Networks offers unlimited access to [gsnetworks.org](http://gsnetworks.org) program deliverables including project plans, research publications and multi-media presentations, all posted for member use, review and feedback. Webinars on current research are held quarterly. Please visit our web site at [www.gsnetworks.org](http://www.gsnetworks.org) or contact [info@gsnetworks.org](mailto:info@gsnetworks.org) for information on participation.



Ten Types of Global Solution Networks