Mapping online child safety in Asia and the Pacific

Rajnesh D. Singh

Internet Society Asia-Pacific, Asia-Pacific Bureau, 9 Temasek Blvd Suntec Tower Two #09-01, Singapore 038989, Singapore

Correspondence
Rajnesh D. Singh, Internet Society Asia-Pacific, Asia-Pacific Bureau, Singapore, Singapore.
Email: rajnesh.singh@gmail.com

Funding information
Google; Internet Society

Abstract
In today’s age, the Internet has become essential for children’s education and social development. Yet the very same technologies can expose children to online harm, which can negatively impact their well-being and safety. These risks are becoming more serious as Internet penetration rises, particularly in emerging countries that have limited resources and capacities to tackle complex issues such as online sexual abuse, cyberbullying, and Internet addiction. As research on the entire range of risks that children are exposed to online is limited, particularly in Asia and the Pacific, this study aims to initiate the process of filling this knowledge gap and proposes a set of policy recommendations to address the challenge of balancing children’s online opportunities and risks. A key finding from the study is the need for a multistakeholder and collaborative approach to ensure the online safety of children, which must include children themselves.

KEYWORDS
Asia Pacific, child protection, child safety, cyberbully, Internet
INTRODUCTION

The 2030 Agenda for Sustainable Development envisages a world in which every child\(^1\) grows up free from violence and exploitation and strives to provide children with a nurturing environment for the full realisation of their rights and capabilities.

The environments where children are commonly nurtured are in families, communities, and schools, but we can no longer ignore the online environment where children from less than 1 year old are interacting in on a regular basis and for longer periods of time (Croll, 2016). In northern Europe, some markets are reaching saturation with nearly 100% Internet penetration among children (Croll, 2016).

As the Internet, particularly mobile broadband, becomes more accessible and affordable in Asia and the Pacific, the above-mentioned trend—of more children going online for longer periods—is also becoming evident in the region. In India, it is estimated that 134 million children have mobile phones (UNICEF, 2016a). In Indonesia, roughly 60% of children access the Internet through mobile devices (GSMA & NTT DOCOMO, 2012). In the Philippines, around half of the 44 million Internet users are children aged 17 years and below (UNICEF, 2016c). In Thailand, 58% of children aged 6–14 years are using the Internet (Jaroonsaksit, 2016). A study conducted by the China National Youth Palace Association in 2014 in 18 cities found that 72% of children aged 10 years or under in China own a mobile phone, and 30% of children under 6 years have used a tablet. It noted that age 10 is the turning point when children use the Internet not only for online gaming but also for entertainment, communication, learning, and self-expression. By age 13, children become not only online content consumers but also creators (Ng & Ho, 2015).

The Internet is providing unprecedented opportunities for children’s education and social development. For instance, for children with disabilities, the Internet offers valuable tools for accessing services and content that they are unable to access in the physical world. For marginalised children, the Internet enables them to form or be part of online communities that help to develop a sense of collective identity and belonging and overcome forms of discrimination and exclusion. The Internet, together with mobile and location-aware technologies, is also helping to enhance the safety of children.

Yet the very same technologies can expose them to online harm, which can negatively impact their well-being and safety. The risks that children encounter on the Internet are diverse, but they can be divided into three groups (LSE, 2015):

- **Content**—The types of content that children encounter online may be inappropriate, potentially dangerous, and illegal, such as websites that promote self-harm, hate speech, pornography, and violence.
- **Usage/conduct**—The way that children use the Internet may put them at risk. This includes the types of content that children create and share with others. The risks range from cyberbullying, sexting,\(^2\) fraudulent transactions, to privacy and security concerns. Internet

---

\(^1\)In this article, UNICEF’s definition of “child” is used, which refers to a person who is under 18 years old except for any country that legalised the concept of adulthood younger than the standard.

\(^2\)Sexting is the self-production of sexual images that is shared through mobile phones and/or the Internet. Sexting makes children vulnerable to becoming victims of sexual extortion, cyberbullying, and sometimes having their picture copied or used in collections of child sexual abuse material.
addiction, mainly as a result of gaming and online social interaction, is also a concern for many countries.

- Interaction/communication—Interacting with individuals especially on social media networks and chatrooms can expose children to risks such as online grooming, and arranging to meet with potentially or actually abusive strangers.

These risks are becoming more serious as Internet penetration rises, particularly in emerging countries that have limited resources and capacities to tackle these complex issues. Yet comprehensive research on the entire range of risks that children are exposed to online is limited, particularly in Asia and the Pacific. This study aims to initiate the process of filling this gap by conducting a qualitative analysis of secondary data, including a literature review. The analysis focused on the legislations and policies that Asia-Pacific countries have adopted to address the different aspects of online child safety and on the different actors involved in tackling online child safety issues in the region.

Based on the analysis, a set of policy recommendations is proposed to address the challenge of balancing the opportunities and risks for children on the Internet—that is, maximising the opportunities the Internet offers to children’s education and social development and minimising the risks.

2 | METHODOLOGY

To frame the analysis, this study divides Asia-Pacific countries into three clusters by Internet penetration level (high, moderate, and low), which generally has a positive correlation with the income level of a country. Fourteen countries—four to five countries per cluster—have been selected based on the ease of obtaining information on online child safety (see Figure 1 and Table 1).

Using these three clusters of countries, a qualitative analysis of secondary data, including a literature review, was undertaken to identify common issues and challenges related to different aspects of online child safety and examine the priority policy responses and actions that countries within and across clusters have adopted.

The study is based on secondary research online, using key search terms related to online child safety and protection (see Table 2). The key terms are assembled with the country’s name, for example, “child online safety Australia” and “child online policy Malaysia.”

Both academic and nonacademic sources were used in the analysis. Nonacademic sources include reports, websites, presentations, news articles, and blogs by United Nations agencies, and governmental and non-governmental organisations.

3 | THE ONLINE RISKS CHILDREN ENCOUNTER

As mentioned in Section 1, the risks that children encounter on the Internet can broadly be divided into three categories—content, usage/conduct, and interaction/communication. This section will look at each category in turn, highlight evidence of the key issues faced by countries in Asia and the Pacific, and identify gaps in our understanding of emerging issues.

---

3Online grooming for sexual purposes is the process of establishing/building a relationship with a child, using the Internet or other digital technologies to facilitate either online or offline sexual contact.
Literature on content-related risks focuses mainly on children’s exposure to pornography and violence and their impact on children’s values, attitudes, and behaviours. However, a pressing content-related issue that needs greater attention is the rise of fake news and content that promote self-harm and hate speech. Children get a huge amount of information from their social media feeds, where false, exaggerated, or sponsored content is often prevalent. Besides research on understanding how misinformation spreads on social media, research on how children consume and respond to such content and the impact of such content on children is lacking.
A broader issue is the significant increase in child sexual abuse material. This is a serious concern that has magnified with the growth of the Internet. INHOPE (2014), the association of Internet hotlines, found about 84,000 websites containing child sexual abuse material in 2014, a 71% increase from 2013. But many more are being circulated by offenders through hidden platforms, such as file sharing networks (including peer to peer), the “darknet” or similarly encrypted software techniques such as the onion router (TOR; ECPAT, 2017b).

The international community is converging over the need to restrict the proliferation of child sexual abuse material online. Already a number of legal acts and directives obligate Internet service providers to take measures to remove or disable access to child sexual abuse material that is hosted on their service. However, such strategies are bound to be less effective as offenders move to hidden environments, such as the darknet or TOR to share, exchange, and access these materials online. Further research is required on strategies that can be employed to identify offenders that hide behind TOR and other encrypted networks to actively abuse children.

3.2 | Usage/conduct

Cyberbullying appears to be a widely recognised concern. A global survey on cyberbullying of over 7,600 children and youth (aged 8–17 years old) in 25 countries revealed that the highest rate of cyberbullying is in Asia—China (70%), Singapore (58%), and India (53%). China and Singapore were also the only countries to report a higher rate of online bullying than face-to-face bullying. Other Asian countries that reported lower levels of cyberbullying include—Malaysia (33%), Pakistan (26%), and Japan (17%; cited in UNESCO, 2015).

Sexting is another serious concern that has been documented. In Australia, the first comprehensive research into image-based abuse published in May 2017 found that the rate of victimisation was particularly high among young people. One in three teenagers aged 16 to 19 and one in four aged 20 to 29 reported having had sexual or nude images taken or distributed online without their consent or used against them (Henry, Powell, & Flynn, 2017).

An emerging concern that is starting to gain attention is the impact of the Internet of Things on the privacy and security of children. Companies that produce and manage the digital products that make up the rapidly growing Internet of Things are all collecting and using personal data. These include games and apps targeted at enhancing play and learning, smart toys that connect to the cloud to analyse, process, and respond to children’s conversations and images, and GPS-enabled wearables such as smart watches. These are all exposing children to various risks including data theft, unlawful surveillance, commercial exploitation, and possibly even sexual exploitation.

Increasingly, smart technologies to engage with children are being developed by companies that are not focused on the technological aspects. In fact, many are small and specialised companies that neither have the resources nor the diligence to put in place privacy and security safeguards. For instance, the microprocessors in smart toys often do not have the processing power required for strong security measures and secure communication, such as encryption. Some smart toys are found to transmit data in clear text (Oxford Internet Institute, 2017).

The implications on children’s rights, privacy, and protection, the ethics of the capture and management of children’s data, and the potential for commercial and sexual exploitation all require more attention.
3.3 Interaction/communication

Social media and messaging tools are often the means by which children first encounter the Internet, and it is on these platforms that they are exposed to many of the risks on cyberspace. As mentioned in Section 3.1, social media has transformed how society creates and consumes news and information, and Section 3.2 brings to attention the use of social media to bully and shame others. Additionally, it has allowed for new ways to recruit victims and facilitate people trafficking. For example, it is estimated that nearly one quarter of children reported missing in Indonesia had been lured into trafficking by their captors through Facebook (MTV Exit cited in A. R. Mubarak, 2015).

A UNICEF study (2016b) revealed that when online threats occur, more adolescents turn to friends rather than parents or teachers, but less than half of the adolescents (41%) strongly agree that they know how to help a friend in these circumstances. Even in Australia where there is a national programme to educate children on online safety and a dedicated helpline for children, a study showed that only 41% of children who were cyberbullied between 2015 and 2016 took action, that is, told their parents or friends, or blocked the person (Australian Government Office of the eSafety Commissioner, 2016). Therefore, empowering children to protect themselves and their peers from online risks is a priority action. At the same time, parents, guardians, caregivers, and educators need to be included in online safety awareness and education efforts as they have varying levels of awareness of the risks online and, as nondigital natives, often struggle to keep up with the ever-changing online techniques being used to target and harm children that are in their care.

Similarly, law-making and enforcement authorities, as well as all child protection stakeholders are seriously challenged by the emerging online techniques used to target and harm children as online products, services, and technologies are developing at a rapid pace. According to a global survey of 370 police officers in 26 countries, including Australia, India, Republic of Korea, New Zealand, and the Philippines, anonymisation and encryption are the top challenges of police investigations on online child sexual abuse and exploitation (NetClean, 2016). It is therefore vital to enhance our understanding of how offenders are using anonymisation and encryption techniques and work with relevant experts to explore opportunities to prevent their use for illegal activities.

4 LEGISLATIONS, POLICIES, AND PROGRAMMES ON ONLINE CHILD SAFETY

A review of the legislations, policies, and programmes in place in the selected countries with different levels of Internet penetration suggests that countries with high Internet penetration have relatively strong legislations and policies to address a variety of online child safety issues.

Some examples given below show that these countries with high Internet penetration have adopted both a top-down approach with legislations to limit and respond to children’s exposure to online harm and a bottom-up approach that enables children, parents, and educators to take charge of minimising the dangers that children face online.

As these are generally high-income countries, the public sector tends to be better resourced to lead and coordinate online child safety issues. For example, in Australia, the Office of the eSafety Commissioner was established in 2015 to focus and coordinate efforts on online child
safety issues. Most of the actors in these countries are from the public sector, but many of the initiatives involve public–private–civil society partnerships.

Countries with high Internet penetration are also more likely to have a broad strategy for empowering children to protect themselves online, with government agencies, the private sector, and civil society working together to provide young Internet users the skills and tools they need to take control of their well-being and strengthen their resilience to risks on the Internet.

Middle- and low-income countries that tend to have moderate and low Internet penetration, respectively, typically do not have as much resources at their disposal. In these countries, the public sector has taken initiatives to address online child safety issues through legislations and policies, albeit less rigorously than those with high Internet penetration. But international non-governmental organisations such as End Child Prostitution and Trafficking, INHOPE, and the International Centre for Missing and Exploited Children (ICMEC), as well as United Nations agencies such as UNICEF and UNESCO, have stepped up to provide support in raising awareness and conducting research to inform policymaking.

These countries with moderate and low Internet penetration have mainly focused their efforts and resources on addressing online child sexual abuse and exploitation through a range of measures—legal, policy, technical, social, and educational. But they are starting to more actively support digital skills and safety training for children, although these efforts tend to be stand-alone initiatives.

It is worth noting that mechanisms have been put in place in some moderate and low Internet penetration countries to focus on online child safety issues and on public–private–civil society partnerships to address these issues. For example, Malaysia has a Child Online Protection Taskforce, led by the Ministry of Women, Family and Community Development. The Philippines has an Inter-Agency Council Against Child Pornography composed of 12 governmental and three non-governmental organisations. In India, the National Advisory on Preventing and Combating Cyber Crime against Children, prepared in 2012, provides a set of guidelines to help state agencies minimise cases of cybercrime against young Internet users. The Indian government is also planning to establish a National Cyber Crime Coordination Centre with a dedicated unit for cyber offenses against women and children.

4.1 | Online sexual abuse and exploitation

Countries, regardless of their level of Internet penetration, are working to protect children from online sexual abuse and exploitation and criminalise the production and distribution of child pornography under domestic law.

However, the quality of legislation varies. Countries with high Internet penetration tend to have a clear and consistent definition of “child” and “child pornography,” include offenses facilitated by all Internet-enabled platforms, and incorporate mental health and medical services for child victims. Australia, New Zealand, and Singapore, as well as some countries with moderate and low Internet penetration, including Malaysia, Philippines, and India have gone a step further, introducing legal measures to deal with offenses related to online child grooming (ICMEC, 2017). Preventing online grooming is important as it often precedes the creation or distribution of child pornography. Targeted legislation may help to prevent latent or previously undetected sex offenders from targeting children. In 2017, ICMEC published a global review and model legislation for preventing online grooming of children and equipping law enforcement agencies with the authority to investigate and prosecute offenders (ICMEC, 2017).
In most countries with moderate and low Internet penetration, however, the definitions, age of consent to sexual relations, and type of offenses are not consistent with international legal standards. These are key barriers to extraditing and prosecuting transborder crimes, due to the "dual criminality" clause—extraterritorial legislation that requires an act to be a crime in both the country where it took place and the country where the suspect resides.

The main international legal instrument that addresses online child sexual abuse and exploitation is the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC). As of 2016, most countries in the Asia-Pacific region have legislation specific to child pornography that are more or less in line with the OPSC, except for Afghanistan, Iran, Kiribati, Democratic People's Republic of Korea, Maldives, Marshall Islands, Micronesia, Nauru, Nepal, Pakistan, Palau, Samoa, Solomon Islands, and Tuvalu (ICMEC, 2016).

The OPSC was adopted in 2000, but since then, new forms of online threats have emerged that are increasing the amount of child sexual abuse material online (see Table 3). For example, the Philippines' legal framework to protect children against sexual abuse and exploitation meets almost all the requirements of ICMEC's model legislation (ICMEC, 2016). Yet the live streaming of child sexual abuse in the Philippines has emerged and become an escalated concern (Holmes, 2016; UNICEF, 2017; Varrella, 2017).

Child pornography is a transnational problem that demands a global response. It is important to harmonise national and international legal standards as inconsistent policies weaken

---

**TABLE 3** Strengths and weaknesses of the OPSC (ECPAT, 2017a)

| Strengths of the OPSC | Weaknesses of the OPSC |
|-----------------------|------------------------|
| • Promotes a holistic approach addressing underlying causes such as poverty; this includes, for example, prevention, awareness raising, and reporting obligations. | It does not specifically define and criminalise all conducts related to online child sexual abuse and exploitation, namely: |
| • It contains provisions concerning jurisdiction, extradition, and mutual assistance to further facilitate and enhance international cooperation. | • Knowingly accessing or viewing child sexual abuse material. |
| • It criminalises those attempting, complying, or participating in the conduct, which can be used to prosecute offenders and facilitators. | • Merely possessing child sexual abuse material. |
| • It calls for measures to protect the rights and interests of child victims at all stages of the criminal justice process. | • Digitally generated child sexual abuse material.a | |
|                       | • Online grooming for sexual purposes. |
|                       | • Sexual extortion or sextortion.b |
|                       | • Live streaming of online child sexual abuse. |

*a*In digitally generated child sexual abuse material, the production of the material does not involve actual contact abuse of real children but is artificially created using digital tools to appear as if real children are depicted. Although such material does not involve harm to a real child, it is still dangerous because (a) it may be used in grooming children for sexual exploitation; (b) it sustains a market for child sexual abuse material; and (c) it enables a culture of tolerance for the sexualisation of children and cultivates demand.

*bSextortion is defined as threats to expose a sexual image to make a person do something (continue to produce sexual material, perform sexual acts, pay money) or for other reasons, such as revenge or humiliation.

---

4Note that the Philippine Anti-Child Pornography Act of 2009 is in accordance with international frameworks, except for the mandatory filtering provision.
prevention and prosecution efforts and allow child predators to target countries where they would be best able to exploit children.

To promote coordination and cooperation among Asia-Pacific countries in tackling online sexual abuse and exploitation of children, as well as other online child safety issues, countries with high Internet penetration and increasingly those with moderate Internet penetration are joining global and regional networks to support their domestic initiatives. They include the following:

• ITU-ASEAN Child Online Protection Strategy Framework is being developed in line with the Association of Southeast Asian Nations Information and Communications Technology Masterplan 2020. It aims to harmonise legislative frameworks on online child protection, promote multistakeholder collaboration, and develop a comprehensive capacity building programme for different stakeholders.

• Association of Southeast Asian Nations Regional Plan of Action on the Elimination of Violence against Children, approved in 2015, includes the development of preventive measures against online violence as a priority action.

• Asia-Pacific Financial Coalition Against Child Pornography, an initiative of the International Centre for Missing and Exploited Children, launched in 2009, aims to fight against the online sale and dissemination of child sexual abuse material. Members include banks, credit card companies, online third-party payment systems, technology companies, social networking platforms, industry associations, and law enforcement agencies.

• ITU Child Online Protection Initiative, launched in 2008 as part of the International Telecommunication Union Global Cybersecurity Agenda Framework, is a multistakeholder effort to promote online child safety.

• Dynamic Coalition for Child Online Safety of the Internet Governance Forum aims to create an open avenue for the discussion of issues related to online child safety.

• WePROTECT Global Alliance is a worldwide cooperation to stop online child sexual abuse and exploitation.

• Virtual Global Taskforce for Combating Online Child Sexual Abuse is an international alliance of law enforcement agencies, non-governmental organisations, and industry players.

4.2 | Other online risks

Countries with high Internet penetration have enacted laws and developed interventions on other aspects of online safety, such as children’s exposure to harmful content, cyberbullying, sexting, and Internet addiction.

4.2.1 | Harmful online content

Very often, countries have used filtering techniques to minimise access to harmful content online. A UNESCO survey (2016) found that 80% of Asia-Pacific countries employ filtering and/or monitoring systems at the local, provincial, and/or national levels to deal with the online risks faced by children. Yet many countries do not have assessment programmes in place to measure the efficacy of their policies and procedures. In Japan, the Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People compels businesses related to the Internet to filter content harmful to children. These businesses, including Internet
service providers and content hosts, can play an important role in developing and using technical solutions such as PhotoDNA image hashing, machine learning, and big data analytics to sort through massive quantities of files and facilitate the processes of identification, removal, filtering/blocking, and reporting child sexual abuse material (Ith, 2015).

### 4.2.2 | Cyberbullying

Recently, Australia, New Zealand, the Philippines, and Singapore have passed laws to protect children against cyberbullying. But because children are often the perpetrators of cyberbullying, these laws face criticism for criminalising children and for being inconsistent with the right to freedom of expression. Some critics believe that it is more effective to tackle cyberbullying through awareness raising and education programmes with parents, guardians, and schools (Berg & Breheny, 2014). Studies from Australia and Thailand have provided evidence that online and offline bullying are closely interlinked, which suggests that prevention programmes should tackle both as interconnected problems (UNESCO, 2015).

Australia has established an Office of the eSafety Commissioner that provides online safety education for Australian children as part of the National Safe Schools Framework, has a complaints service and kids helpline for young Australians who experience cyberbullying, and addresses illegal online content.

### 4.2.3 | Sexting

Sexting, when it occurs between two consenting individuals, is not an act of cyberbullying but has emerged as a related issue when images are used to blackmail, stalk, or ruin others’ reputations or can at times be considered as child sexual abuse material. A study in Queensland, Australia, revealed that young people have been inadvertently creating illegal child sexual abuse material through sexting and in response, the Queensland Police has formally adopted a policy that emphasises education over punishment. The study found that almost half (1,498) of the 3,035 offenders dealt with by the criminal justice system in Queensland for child sexual abuse material over the past decade were children (under 17 years old). The trend of engagement with sexting-based offences has been increasing with 331 young offenders cautioned during 2015–2016, compared with only 28 in 2006–2007. Findings from this study prompted the Queensland Police to incorporate guidelines on how to handle teenagers’ sexting into its Operational Procedures Manual (Hunt, 2017).

### 4.2.4 | Internet addiction

In the Republic of Korea, Chapter 3 of the Juvenile Protection Act passed in 2014 deals with preventing juvenile addiction to Internet games. In addition, Article 23 of the Act aims to protect children from harmful content online. Chapter 3 consists of four articles on Internet addiction:

- Article 24 requires a parental authority’s consent prior to a minor’s use of Internet games;

---

6 Under Queensland law, child sexual abuse material includes that which depicts a person under 16 years old in a sexual context.
• Article 25 requires Internet game providers to specify the game’s appropriateness for a particular age group and inform parents or legal guardians on any payments related to the product;
• Article 26 restricts the provision of Internet games to juveniles under the age of 16 between 12 midnight and 6 am; and
• Article 27 details the support available for juveniles afflicted with addiction to Internet games.

Other countries in the region, such as China and Viet Nam, have begun to address Internet addiction through measures such as rehabilitation programmes and by limiting permissible hours for children in Internet cafes.

5 | POLICY RECOMMENDATIONS

Based on the study, a number of policy recommendations are proposed.

• In domestic laws, clearly define terms based on international legal standards and include offenses facilitated by all Internet-enabled platforms. Harmonisation of terminology used is critical.

Terms such as “child,” “child pornography,” and “online grooming” should be clearly defined where relevant based on the OPSC and guidelines from relevant international bodies. It is also important to explicitly criminalise online grooming and include offenses facilitated by all Internet-enabled platforms in national law.

• Ensure that policies to protect children online are consistent with other important policy objectives, such as the preservation of fundamental rights, including freedom of expression and privacy.

Measures that prevent and mitigate risks should not reduce the benefits of the Internet for children and should be consistent with the United Nations Convention on the Rights of the Child, which were signed and ratified by all countries in Asia and the Pacific. These fundamental values include the right of children to freedom of expression and privacy.

For example, filtering and blocking techniques have been criticised for limiting access to information and preventing valued peer support, as some filters can remove legitimate content and forums that cover topics such as health and sexuality. It has been argued that these measures may serve as a smokescreen to justify wider forms of censorship and repression of free speech. Transparency is therefore important in measures that involve content filtering. Information about how a site gets on—or off—a filtered or blocked list should be made available. Lists should also be consistently reviewed and updated.

Moreover, there does not seem to be any targeted legislative response to the online privacy of children and the protection of children from information security risks. Research on these aspects are urgently needed.

• Collaborate, adopt a multistakeholder approach, and ensure international cooperation.
Attention should be focused on how to make the Internet safer for everyone by adopting a multistakeholder and collaborative approach in which the burden to anticipate and cope with online risks do not fall entirely on children and parents but stakeholders from the private sector and government should also take responsibility for ensuring online safety. Relevant stakeholders include the following:

| Children and youth                          | Parents and guardians          | Schools and education sector |
|---------------------------------------------|--------------------------------|------------------------------|
| Legislators, policymakers, and regulators  | Law enforcement agencies       | Health sector                |
| Internet service providers and mobile network operators | Privacy, security, and encryption experts | Social media and messaging platforms, and search engines |
| Owners of public access points, for example, Internet cafés, telecentres, and online gaming centres | Companies developing products and providing services to children, families, and schools | Financial sector |
| Child protection and welfare organisations  | International alliances and networks | Academic and research institutions |

- Make digital citizenship a priority in online child protection policies.

Policymakers need to acknowledge children's capacity to protect themselves and combat the risks that they encounter on the Internet. Legislations to minimise harm should be balanced with measures that make available knowledge and tools and develop habits and attitudes to build children's resilience, while enabling them to engage constructively online.

Digital literacy training should thus not only equip children with technical skills but also seek to instil responsible behaviour. This includes exercising care in the content they create, the information they share with others, and their interaction with other children and with adults, especially strangers in cyberspace.

- Develop a coordinated strategy for awareness raising and education on online child safety for different actors.

Efforts to promote digital citizenship should be undertaken alongside measures to encourage parents, guardians, caregivers, and educators to guide and assist young Internet users in safely navigating the Internet, especially in recognizing and reporting online grooming and dealing with cyberbullying and sexual extortion.

Many countries have implemented activities to raise awareness on online child safety issues among children, parents, educators, and even industry, but they are often ad hoc activities. A coordinated approach and strategy would enable stakeholders to pool resources and expertise for greater impact.

There are diverse groups of children of different ages, ethnicity, ability, socio-economic positions living in urban or rural settings. Public awareness and education materials on online child safety need to be tailored to suit the different groups of children.

Empowering older children to act as mentors and guides to younger users could be effective as a peer support mechanism. Children may find it easier to discuss some issues with those of a similar age (e.g., senior/older students) rather than adults. This could be implemented in schools along with digital literacy programmes.
Engage with children to develop robust research on online child safety and integrate findings in child protection systems.

In 2016, UNESCO surveyed 22 countries in the Asia-Pacific to review their capacity to foster digital citizenship among children. The findings revealed that two thirds of these countries involved multiple sectors, such as law enforcement, health, education, and security, in developing cybersafety and privacy policies. What was missing were initiatives to engage with children to gain a better understanding of their perspectives on the opportunities and risks of the Internet and other digital tools. The lack of rigorously obtained data on children’s behaviours and perceptions online, potentially lead to the development and implementation of policy based on general and untested assumptions (UNESCO, 2016).

Children are a vital stakeholder in addressing issues of online safety. It is thus important to embed children’s voices and concerns in developing and implementing new digital resources and ensure that business-led innovation is subject to effective national and international regulation that recognises children’s rights and is informed by risk impact assessments.

Research related to the use/consumption and impact of the Internet of Things and artificial intelligence in games, apps, smart toys, and wearables, as well as fake news and content that promote self-harm on children should be a priority.

Strengthen the child protection and technological capacity of law enforcement agencies.

Law enforcement agencies do not always view online sexual abuse and exploitation as a child protection issue. In many countries, it is regarded as a “cybercrime” and officers may therefore have little or no expertise, or professional interest in child protection. It is therefore important for law enforcement agencies to be aware and sensitive to aspects of online child safety and have the will and capacity to work with other stakeholders. An understanding of the fast-changing Internet ecosystem is needed, as well as expertise in areas such as digital forensics. Research on techniques to identify offenders that hide behind TOR and other encrypted networks to abuse children and share child sexual abuse materials should be a priority.

Develop consistent indicators to assess and monitor online child safety.

There is limited statistical data on children’s use of the Internet and the risks that they face online. Findings from various studies are rarely comparable. International cooperation would benefit from consistent indicators to measure online child safety. Countries may refer to existing guidelines, such as the ITU’s Child Online Protection Statistical Framework and Indicators.

ORCID

Rajnesh D. Singh http://orcid.org/0000-0003-3630-7701

REFERENCES

Australian Government Office of the eSafety Commissioner (2016) Research insights: Teens, Kids and Digital Dangers.

Berg, C., & Breheny, S. (2014). Enhancing online safety for children. Institute of Public Affairs, Australia.
Croll, J. (2016). Let’s play it safe: Children and youths in the digital world—assessment of the emerging trends and evolutions in ICT services. White Paper for the ICT Coalition for Children Online, 11 January.

ECPAT (2017a). Online child sexual exploitation: A common understanding. Bangkok.

ECPAT (2017b). Online child sexual exploitation: An analysis of emerging and selected issues. ECPAT International Journal, (12; 8). (April).

GSMA, & NTT DOCOMO (2012). Children’s use of mobile phones: An international comparison.

Henry, N., Powell, A., & Flynn, A. (2017). Not just ‘revenge pornography’: Australians’ experiences of image-based abuse—A summary report. RMIT University.

Holmes, O. (2016). How child sexual abuse became a family business in the Philippines. The Guardian, 31 May.

Hunt, E. (2017). Sexting to blame for nearly 1,500 children convicted for child exploitation. The Guardian, 9 May.

ICMEC (2016). Child pornography: Model legislation and global review, 8th edition.

ICMEC (2017). Online grooming of children for sexual purposes: Model legislation & global review, 1st edition.

INHOPE (2014). Infographic on online child abuse material.

Ith, T. (2015). Microsoft’s PhotoDNA: Protecting children and businesses in the cloud. Microsoft, 15 July.

ITU (2017). Statistics: Country ICT data (Until 2016). http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (accessed on 6 November 2017).

Jaroonsaksit, R. (2016). Kingdom of Thailand: Child online protection initiatives. Presentation made on 13 September for ITU.

LSE (2015). Children’s safety on the Internet: A guide to stakeholders. London School of Economic and Political Science (LSE) Media Policy Project Blog, 31 March.

Mubarak, A. R. (2015). Child safety issues in cyberspace: A critical theory on trends and challenges in the ASEAN region. International Journal of Computer Applications, 129 (November), 48–55.

NetClean (2016). The NetClean report 2016.

Ng, K. C., & Ho, B. C. (2015). APrIGF 2015 workshop report.

Oxford Internet Institute (2017). How and Why is children’s digital data being harvested. 10 May.

UNESCO (2015). From insult to inclusion: Asia-Pacific report on school bullying, violence and discrimination on the basis of sexual orientation and gender identity. Bangkok.

UNESCO (2016). A policy review: Building digital citizenship in Asia-Pacific through safe, effective and responsible use of ICT. Bangkok.

UNICEF (2016a). Child online protection in India. New Delhi.

UNICEF (2016b). Perils and possibilities: Growing up online.

UNICEF (2016c). Globe, UNICEF Philippines, Ateneo Sign MoU on online child protection.

UNICEF (2017). UNICEF study: 8 in 10 Filipino youth in danger of online sexual abuse. 7 June.

Varrella, A. (2017). Live streaming of child sexual abuse: Background, legislative frameworks and the experience of the Philippines. ECPAT International Journal, (12; 47). (April).

The opinions expressed in the Policy Forum are those of the author(s) alone and do not necessarily reflect those of the Journal’s Editors and partners.

How to cite this article: Singh RD. Mapping online child safety in Asia and the Pacific. Asia Pac Policy Stud. 2018;5:651–664. https://doi.org/10.1002/app5.247