Issue Paper: Asia-Pacific Bureau
Digital Safety of Children and Youth

November 2017

This issues paper builds on two Internet Society reports, ***"Children and the Internet"*** [1] and ***"Mapping Online Child Safety in Asia-Pacific"*** [2] to discuss the challenges and opportunities related to the digital safety of children and youth in the Asia-Pacific region.

The Issues

Children and youth are faced with increasing risks and threats on the Internet that can cause serious harm

The Internet brings opportunities for children's education, self-expression and social development. But its use also exposes children to various risks related to:

- Cyberbullying;
- Online fraud;
- Inappropriate, potentially dangerous and illegal sites with content on pornography, violence, self-harm, racial hatred, etc.;
- Online sexual abuse and exploitation; and
- Cyberaddiction, mainly as a result of overuse of technology for gaming and social interaction.

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%).[3]

[1] Internet Society, "Children and the Internet," 2012, https://www.internetsociety.org/children-and-internet.

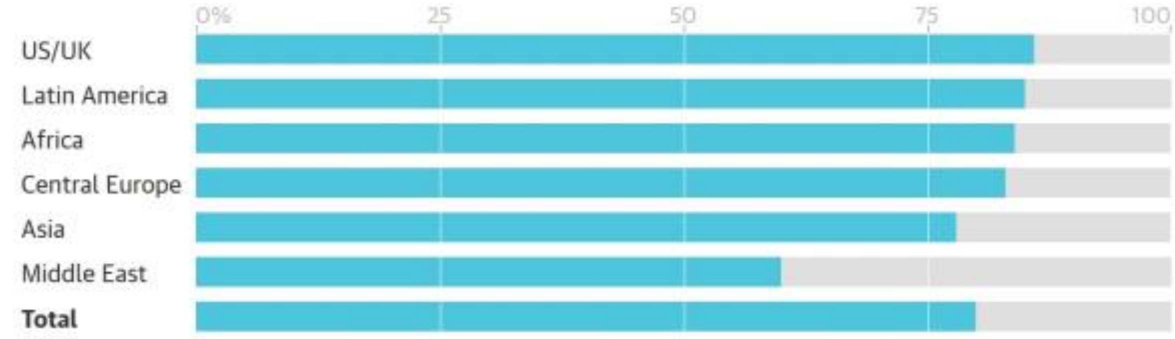
[2] Internet Society, "Mapping Online Child Safety in Asia-Pacific," July 2017, https://www.internetsociety.org/doc/mapping-online-child-safety-asia-pacific.

[3] Cited in UNESCO, *From Insult to Inclusion: Asia-Pacific Report on School Bullying, Violence and Discrimination on the Basis of Sexual Orientation and Gender Identity* (Bangkok, 2015), http://unesdoc.unesco.org/images/0023/002354/235414e.pdf.

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%).

Around 78% of 18-year old Asians believe young people are in danger of being sexually abused or taken advantage of online, according to a global survey commissioned by UNICEF.[4]



Source: Oliver Holmes, "Most 18-year-olds say young people at risk online, Unicef poll finds," The Guardian, 7 June 2016,

Social media and messaging tools are often the means by which children and young people first encounter the Internet, and it is on these platforms that they are exposed to many of the risks on cyberspace. 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.[5]

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.[6]

In Australia, the first comprehensive research into image-based abuse published in May 2017[7] 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.

Summary of findings from the Internet Society report, “Mapping Online Child Safety in Asia-Pacific”[8]

- Countries, regardless of their level of Internet penetration, are working to protect children from online sexual abuse and exploitation, but at varying degrees.

[4] UNICEF, "Perils and Possibilities: Growing Up Online," http://www.unicef.org.hk/upload/NewsMedia/publication/UNICEF_Growing-up-online.pdf; and UNICEF Hong Kong, "In Asia, 78 per cent of 18-year-olds believe young people are in danger of online sexual abuse," 7 June 2016, http://www.unicef.org.hk/en/in-asia-78-per-cent-of-18-year-olds-believe-young-people-are-in-danger-of-online-sexual-abuse-unicefipsos-global-poll/.

[5] MTV Exit cited in A. R. Mubarak, "Child Safety Issues in Cyberspace: A Critical Theory on Trends and Challenges in the ASEAN Region," *International Journal of Computer Applications*, Vol. 129, No. 1 (November 2015), pp. 48-55, http://www.ijcaonline.org/research/volume129/number1/mubarak-2015-ijca-906925.pdf.

[6] UNICEF, "Perils and Possibilities: Growing Up Online," http://www.unicef.org.hk/upload/NewsMedia/publication/UNICEF_Growing-up-online.pdf.

[7] Nicola Henry, Anastasia Powell and Asher Flynn, "Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse - A Summary Report," RMIT University, May 2017, https://www.rmit.edu.au/content/dam/rmit/documents/college-of-design-and-social-context/schools/global-urban-and-social-studies/revenge_porn_report_2017.pdf.

[8] Internet Society, “Mapping Online Child Safety in Asia-Pacific,” July 2017, https://www.internetsociety.org/doc/mapping-online-child-safety-asia-pacific

- Countries with high Internet penetration tend to have a clear and consistent definition of "child" and "child pornography", and include offenses facilitated by all Internet-enabled platforms. But in most countries with moderate and low Internet penetration, the definitions, age of consent to sexual relations and type of offenses are not consistent with international legal standards, which are key barriers to extraditing and prosecuting transborder crimes.

- Countries with high Internet penetration have also enacted laws and developed interventions on other aspects of digital safety, such as children's exposure to harmful content, cyberbullying and Internet addiction.
- To date, there does not seem to be any targeted legislative response to the online privacy and the protection of children from information security risks.
- Comprehensive measures to equip children with the knowledge, tools and skills necessary for them to manage these risks are still lacking in the region.

Internet technologies bring both benefits and threats, and dealing with their misuse/illegal use is a pressing concern

Online products, services and technologies are developing at a rapid pace, bringing about evolving opportunities, but law-making and enforcement authorities, and all child protection stakeholders are seriously challenged by the emerging online techniques used to target and harm children and young people.

Parents and caregivers are increasingly unable to protect their children online, and are consequently becoming more dependent on para-familial structures and organisations to reach and teach their children.

Anonymisation and encryption tools, which are important for ensuring the privacy and security of individuals online, are also being used for harmful and illegal activities.

INHOPE, the association of Internet hotlines, found about 84,000 websites containing child sexual abuse material,[9] 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).[10]

According to a global survey of 370 police officers in 26 countries, including Australia, India, Republic of Korea, New Zealand and the Philippines,[11] anonymisation and encryption are the top challenges of police investigations on online child sexual abuse and exploitation.

Cryptocurrencies and virtual currencies are being used by child sexual abuse offenders and so far, there are limited opportunities to obstruct them.

Cryptocurrencies, like bitcoin, have numerous benefits,[12] but because they allow transactions without the entity at either end disclosing their real identity, they are also being used to trade

[9] INHOPE, Infographic on online child abuse material, http://www.inhope.org/libraries/statistics_infographics_2014/inhope_stats_infographics_for_2014.sflb.ashx.

[10] ECPAT, "Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues," *ECPAT International Journal*, Issue 12 (April 2017), http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf.

[11] NetClean, "The NetClean Report 2016," http://www.netclean.com/wp-content/uploads/2016/12/NetClean_Report_2016_English_print.pdf.

[12] See Ameer Rosic, "7 Incredible Benefits of Cryptocurrency," *Huffington Post*, 23 November 2016, http://www.huffingtonpost.com/ameer-rosic-/7-incredible-benefits-of-_1_b_13160110.html.

child sexual abuse material. Virtual gaming currencies and commodities likewise play a part in online grooming where payments are made to children to gain their trust and/or convince them to share material of a sexual nature.[13]

These avenues, especially when paired with other anonymisation/encryption tools, make it difficult to identify child sex offenders involved in the transaction. Their increased use for malicious purposes represents a new obstacle for law enforcement authorities, who may have to rely on offenders making a mistake for them to be apprehended.[14]

There is a significant knowledge gap on the application of different types of cryptocurrencies for online child exploitation, which makes it difficult to develop preventive responses. A number of emerging online payment services are able to offer even higher levels of anonymity than those currently available.[15] It is therefore vital to enhance our understanding of cryptocurrencies and how they are being used by child sex offenders. It is also important to cooperate with the cryptocurrency sector and encryption experts to explore opportunities to prevent their use for illegal activities.

Countries have yet to balance the safety of children and youth on the Internet with their fundamental rights

Addressing the risks that children face online without reducing their access to the opportunities and benefits of the Internet is a complex global challenge. For example, in Lalpur, a village in the northern state of Uttar Pradesh in India, leaders ordered mobile phones confiscated from every girl under the age of 18 years after a local teacher, who had used a smartphone, was arrested on charges of molesting one of his students.[16]

Content filtering and blocking are common technical solutions, but they should be weighed against the right to information and expression

Very often, countries have used filtering techniques to control access to content. A UNESCO survey[17] 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 do not have assessment programmes in place to measure the efficacy of their policies and procedures.

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 also 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.

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

[13] Yvonne Nouwen, "Virtual Currency Uses for Child Sex Offending Online," *ECPAT International Journal*, Issue 12 (April 2017), http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf.

[14] Ibid.

[15] Ibid.

[16] Eric Bellman and Aditi Malhotra, "Why the vast majority of women in India will never own a smartphone," *The Wall Street Journal*, 13 October 2016, http://www.wsj.com/articles/why-the-vast-majority-of-women-in-india-will-never-own-a-smartphone-1476351001.

[17] UNESCO, *A Policy Review: Building Digital Citizenship in Asia-Pacific through Safe, Effective and Responsible Use of ICT* (Bangkok, 2016), http://unesdoc.unesco.org/images/0024/002468/246813e.pdf.

providers to take measures to remove or disable access to child exploitation content that is hosted on their service.

However, such strategies are bound to be much less effective as offenders move to hidden environments, such as the darknet/TOR, to share, exchange and access these materials online.

Legal responses to cyberbullying and sexting are criminalising children

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.[18]

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.[19]

Sexting,[20] when it occurs between two consenting individuals, is not an act of cyberbullying, but has emerged as a related issue, as images that are shared and re-shared with the intent to harm can have a negative impact on a minor's mental health and social well-being.[21] These images can also be used to blackmail, stalk or ruin others' reputations, or as in the case illustrated below, can at times be considered as child pornography or child sexual abuse material.[22]

Young people are inadvertently creating illegal child pornography through sexting

A study by the Queensland Sentencing Advisory Council in Australia 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). Most of the young offenders were engaged in sexting-related offences and received a formal caution from police. The average age was about 15, with the youngest 10. Under Queensland law, child sexual abuse material includes that which depicts a person under 16 years old in a sexual context.[23]

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 formally adopt a policy emphasising education over punishment, and guidelines on how to handle teenagers'

[18] Chris Berg and Simon Breheny, "Enhancing Online Safety for Children," Institute of Public Affairs, Australia, March 2014, http://ipa.org.au/portal/uploads/submission_to_Enhancing_Online_Safety_for_Children.pdf.

[19] Cited in UNESCO, *From Insult to Inclusion: Asia-Pacific Report on School Bullying, Violence and Discrimination on the Basis of Sexual Orientation and Gender Identity* (Bangkok, 2015), http://unesdoc.unesco.org/images/0023/002354/235414e.pdf.

[20] **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.

[21] Barbara A. Spears, Phillip T. Slee and Jillian Huntley, *Cyberbullying, Sexting and the Law: A Report for the South Australian Minister for Education and Child Development* (Adelaide: University of South Australia, 2015), https://www.unisa.edu.au/Global/EASS/EDS/Research%20Supervisors/Spears,%20Slee,%20Huntley%20Cyberbullying,%20Sexting%20and%20the%20Law.pdf.

[22] **Child sexual abuse material** includes material depicting acts of sexual abuse and/or focusing on the genitalia of the child.

[23] Elle Hunt, "Sexting to blame for nearly 1,500 children convicted for child exploitation," *The Guardian*, 9 May 2017, https://www.theguardian.com/australia-news/2017/may/09/sexting-guidelines-created-by-queensland-police-as-child-convictions-soar.

sexting were incorporated into the Queensland police's Operational Procedures Manual in November 2016.[24]

A robust legal framework is insufficient, and a multi-stakeholder and collaborative approach is required to ensure the safety of children and youth online

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.[25]

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 below).

Strengths of the OPSC	Weaknesses of the OPSC
• Promotes a holistic approach addressing underlying causes such as poverty; this includes e.g., prevention, awareness-raising and reporting obligations. • It contains provisions concerning jurisdiction, extradition and mutual assistance to further facilitate and enhance international cooperation. • It criminalises those attempting, complying or participating in the conduct, which can be used to prosecute offenders and facilitators.	It does not specifically define and criminalise all conducts related to online child sexual exploitation, namely: • Knowingly accessing or viewing child sexual abuse material. • Merely possessing child sexual abuse material. • Digitally generated child sexual abuse material.[26] • Online grooming for sexual purposes.[27]

[24] Ibid.

[25] International Centre for Missing and Exploited Children, *Child Pornography: Model Legislation and Global Review*, 8th edition (2016), http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf.

[26] **Digitally generated child sexual abuse material** encompasses all forms of material representing children involved in sexual activities and/or in a sexualised manner, with the particularity that 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 were depicted.

Although such material does not involve harm to a real child, it is still dangerous because: (1) it may be used in grooming children for sexual exploitation; (2) it sustains a market for child sexual abuse material; and (3) it enables a culture of tolerance for the sexualisation of children and cultivates demand.

[27] **Online 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. Preventing online grooming is important as it often precedes the creation or distribution of child sexual abuse material, in that by the time intent to meet the child has been expressed, s/he is likely to already have been exploited online. Targeted legislation may help to prevent latent or previously undetected sex offenders from targeting children. Australia, Brunei Darussalam, the Philippines and Singapore have introduced legal measures to deal with offenses related to online child grooming.

• It calls for measures to protect the rights and interests of child victims at all stages of the criminal justice process	• Sexual extortion or sextortion.[28] • Live streaming of online child sexual abuse.[29]

Source: ECPAT, “Online Child Sexual Exploitation: A Common Understanding," May 2017.

For example, the Philippines’ legal framework to protect children against sexual abuse and exploitation meets all the requirements of a model legislation.[30] Yet, the live streaming of child sexual abuse in the Philippines has proliferated. A concerted strategy that includes a combination of legal, law enforcement, educational, technical and socio-cultural measures is required.

The live streaming of child sexual abuse in the Philippines[31]

The Philippines has recently been described as "the global epicentre of the live-stream child sexual abuse trade". According to a recent study, this is mainly driven by poverty, English proficiency, increased access to the Internet and affordability of devices, well-established money transfer system, and its perceived lack of conflict with social norms and laws.

Although the Philippines has a robust legal framework to protect children against sexual abuse and exploitation, it has not been sufficient in addressing and preventing its different manifestations. Awareness-raising activities in schools and communities for both children and parents are needed to reinforce social norms that are in line with the rights of the child. Law enforcement agencies need to collaborate with relevant private actors such as Internet service providers, mobile operators, and financial institutions to monitor and report potential violations. Further research and documentation on its extent, nature and impact is also needed to guide future strategies against it.

[28] **Sextortion** 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. Sextortion is a growing form of online abuse that requires serious attention, particularly as more young girls and boys interact online in the Asia-Pacific region. A recent survey conducted in the US shows the devastating impact of sextortion: 1 in 4 victims saw a medical or mental health professional, and 1 in 8 victims moved from their homes for fear of their safety. It also found that more than 40% of those who did report to websites or apps said the responses they received were not helpful. Only 16% of survey respondents reported episodes to police, but some reported being shamed or blamed by police and some who were minors during incidents were threatened with prosecution for producing child pornography. See Janis Wolak and David Finkelhor, "Sextortion: Findings from a Survey of 1,631 Victims," June 2016, https://www.wearethorn.org/sextortion/.

[29] **Live streaming** does not require the actual downloading or storage of the abusive video footage or frames on a device. In principle, therefore, little or no trace of the crime remains, and offenders can more easily avoid detection by law enforcement officials. Moreover, live streaming of child sexual abuse can be carried out in relative secrecy and the child victims can be moved from one hidden location to another so long as there is an Internet connection and a computer, smartphone or other broadcasting device.

[30] International Centre for Missing and Exploited Children, *Child Pornography: Model Legislation and Global Review*, 8th edition (2016), http://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf. Note that the Philippine Anti-Child Pornography Act of 2009 is in accordance with international frameworks, except for the mandatory filtering provision.

[31] Andrea Varrella, "Live Streaming of Child Sexual Abuse: Background, Legislative Frameworks and the Experience of the Philippines," *ECPAT International Journal*, Issue 12 (April 2017), http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf. See also Oliver Holmes, "How child sexual abuse became a family business in the Philippines," *The Guardian*, 31 May 2016, https://www.theguardian.com/world/2016/may/31/live-streaming-child-sex-abuse-family-business-philippines.

> The live streaming of child sexual abuse is likely to accelerate in many parts of the world because of: ease of access, availability of the devices needed to perpetrate the crime, easily generated income for facilitators and children, low risk levels of being caught by law enforcement, low cost of production, and low cost to view the performances.

Partnerships are essential for addressing online safety issues. Relevant actors include:

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

There is a need to broaden engagement with actors from multiple sectors, taking into account the impact of the Internet of Things on the privacy and security of children and young people.

Companies that produce and manage the digital products that make up the rapidly growing Internet of Things[32] 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 young people 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 contrast, 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.[33]

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.

[32] See Issues Paper on the Internet of Things.

[33] Oxford Internet Institute, "How and why is children's digital data being harvested," 10 May 2017, https://www.oii.ox.ac.uk/blog/how-and-why-is-childrens-digital-data-being-harvested/.

There is a need to empower and engage with children and young people, and better understand their behaviour on the Internet.

In 2016, UNESCO surveyed 22 countries in the Asia-Pacific to review their capacity to foster digital citizenship among children.[34] 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 is missing are initiatives to engage with children to gain a better understanding of their perspectives on the opportunities and risks of information and communication technology (ICT). 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.[35]

According to the UNESCO survey, 75% of Asia-Pacific countries have digital literacy training that equip children with technical skills. But it is recommended that they should also seek to instil responsible behaviour online. 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.

The fact that children as young as 10 years old can become active consumers and producers of online content,[36] underlines the importance of empowering children to use the Internet safely and confidently at a younger age.

The Opportunities

There is a growing number of regional and international agreements that promote coordination and cooperation among countries in tackling digital safety issues

- **ITU-ASEAN Child Online Protection Strategy Framework** is being developed in line with the ASEAN ICT Masterplan 2020. It aims to harmonise legislative frameworks on online child protection, promote multi-stakeholder collaboration and develop a comprehensive capacity building programme for different stakeholders.[37]
- **ASEAN 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**, 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 its Global Cybersecurity Agenda Framework, is a multi-stakeholder effort to promote online child safety.

[34] UNESCO, *A Policy Review: Building Digital Citizenship in Asia-Pacific through Safe, Effective and Responsible Use of ICT* (Bangkok, 2016), http://unesdoc.unesco.org/images/0024/002468/246813e.pdf.

[35] Internet Society, "Mapping Online Child Safety in Asia-Pacific," July 2017, https://www.internetsociety.org/doc/mapping-online-child-safety-asia-pacific.

[36] Ng Ki Chun and Bianca Caroline Ho, "APrIGF 2015 Workshop Report," http://www.dotkids.asia/wp-content/uploads/2015/07/APrIGF2015-Workshop-Report.pdf.

[37] Amelia Gowa, "Draft ASEAN Framework on COP," presentation made at the ITU-ASEAN Workshop on Child Online Protection in Manila, Philippines on 13-14 September 2016, http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Sept-COP/Presentation/Draft%20Regional%20Framework%20Recommendations%20Amelia%20Gowa.pdf.

- **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.

Digital tools are being harnessed to protect children online.

Law enforcement agencies, private actors, the technical community, academia and civil society are coming together to protect children online, particularly in developing technical solutions such as PhotoDNA image hashing,[38] machine learning and big data analytics[39] to sort through massive quantities of files,[40] and facilitate the processes of identification, removal, filtering/blocking and reporting child sexual abuse material.[41] Helplines, crowdsourcing and crowdmapping platforms have emerged for citizens to report and help identify perpetrators.[42] Apps are also being developed to reach out and raise awareness of children on Internet safety, and provide them with tools to help them deal with the various dangers they face online.[43]

Alignment with the SDGs

The 2030 Agenda for Sustainable Development envisages a world in which every child grows up free from violence and exploitation, and strives to provide children and youth with a nurturing environment for the full realisation of their rights and capabilities, through safe schools and cohesive communities and families. The SDG 16.2 specifically refers to the ending of abuse, exploitation, trafficking and all forms of violence against and torture of children. Of relevance is SDG 16a, which calls for the strengthening of relevant national institutions, including through international cooperation, to prevent violence and combat crime.

[38] See International Centre for Missing and Exploited Children, "Project Vic," https://www.icmec.org/project-vic/; and Alex Hern, "Facebook launching tools to tackle revenge porn," *The Guardian*, 5 April 2017, https://www.theguardian.com/technology/2017/apr/05/facebook-tools-revenge-porn.

[39] See Partnership for Conflict, Crime & Security Research, "Pioneering New Work in Online Child Protection," http://www.paccsresearch.org.uk/delivering-impact/case-studies/pioneering-new-work-in-online-child-protection/.

[40] According to a 2016 survey by NetClean, many police officers reported that a normal case contains somewhere between 1-3 terabytes (TB) of data, 1-10 million images and thousands of hours of video material. This refers to all the material in a seizure that officers have to sort through in order to find and investigate the child sexual abuse material. A few police officers have answered that they have had cases as large as 100TB, over 100 million images and over 100,000 hours of video material. NetClean, "The NetClean Report 2016," http://www.netclean.com/wp-content/uploads/2016/12/NetClean_Report_2016_English_print.pdf.

[41] For example, Telenor Group partnered with Interpol to create a mobile Internet filter for child sexual abuse content. Telenor Group, "Telenor in Asia: Internet safety on top of the agenda," 2014, https://www.telenor.com/media/inside-telenor/2014/telenor-in-asia-internet-safety-on-top-of-the-agenda/.

[42] See Child Helpline International, https://www.childhelplineinternational.org; International Association of Internet Hotlines, http://www.inhope.org; Internet Watch Foundation, https://www.iwf.org.uk/; and Timo Luege, "Europol Turns to the Crowd to Identify Locations of Child Abuse," *Social Media for Good*, 2 June 2017, http://sm4good.com/2017/06/02/europol-turns-to-the-crowd-to-identify-locations-of-child-abuse/.

[43] Internet Matters, "E-safety app for parents and children," 4 August 2016, https://www.internetmatters.org/hub/esafety-news/new-e-safety-app-for-parents-and-children/.

Questions to Think About

- What are the strategies that can be employed to identify offenders that hide behind TOR and other encrypted networks to actively abuse children?
- In addition to "privacy by design" and "security by design", how could providers of online products and services be convinced to incorporate solutions to minimise the risk and harm to children and young people?
- What are the guidelines for assessing whether new and emerging technologies will have an impact on children and young people’s safety?
- What are the strategies and good practices for ensuring children and young people’s participation in decision-making by government and private actors regarding their online safety and protection?