DISRUPTING HARM IN INDONESIA

Evidence on online child sexual exploitation and abuse

Warning:

Disrupting Harm addresses the complex and sensitive topic of online child sexual exploitation and abuse. At times in the report, some distressing details are recounted, including using the direct words of survivors themselves. Some readers, especially those with lived experiences of sexual violence, may find parts of the report difficult to read. You are encouraged to monitor your responses and engage with the report in ways that are comfortable. Please seek psychological support for acute distress.

CONTENTS

MESSAGE FROM THE MINISTRY OF WOMEN'S EMPOWERMENT AND CHILD PROTECTION

As of 2021, a majority of children between the ages of 12–17 in Indonesia are internet users. We have witnessed – especially at the start of the COVID-19 pandemic – the value of the internet in supporting children's education, keeping them informed about how to stay safe, and ensuring that they maintain their social connections. However, as with any place that children frequent, there are also potential harms that we must keep in mind when children go on line. One of those risks, is on line child sexual exploitation and abuse (OCSEA).

OCSEA is a growing crime around the world and given that offenders rely on digital technology to perpetrate these forms of violence, it is a crime that knows no borders. As such we must ensure that we take every effort to ensure our national systems are well equipped to keep children safe from harm, and to respond effectively if the harm does occur. An effective response requires heavily on evidence to ensure that we are making well-informed decisions for our children.

The Ministry of Women's Empowerment and Child Protection is pleased to see the completion of the *Disrupting Harm in Indonesia* report, which provides us with a comprehensive assessment of the current threat of OCSEA to children and how our national systems are responding. This report comes during a time of increased commitment by the Government of Indonesia to tackle these crimes against children. In 2019, Indonesia adopted the Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN, a sign of our collective resolve to bolster our child protection standards and our capacity to respond. Further, in September 2021, Indonesia adhered to the earlier ASEAN Regional Plan of Action on the Elimination of Violence against Children 2016–2025.

With this strong commitment, along with the latest evidence from this *Disrupting Harm* report, Indonesia is in a strong position to strengthen its policy, legal frameworks, programs, and overall response to OCSEA. The report offers clear recommended actions addressed to various stakeholder groups and it is the Ministry's hope that all relevant sectors can work collaboratively to act on the recommended ways forward. Ending these forms of violence against children is a shared responsibility and cannot be achieved by one sector alone.

The Ministry of Women's Empowerment and Child Protection would like to congratulate ECPAT International, INTERPOL and UNICEF Office of Research – Innocenti, and the Global Partnership to End Violence Against Children on completing this project and looks forward to further accelerating our efforts to tackle these crimes against children and keeping them safe online.

Pribudiarta Nur Sitepu
Permanent Secretar
Ministry of Women Empowerment and Child Protection
Republic of Indonesia

MESSAGE FROM THE END VIOLENCE PARTNERSHIP

Our online lives are advancing constantly. The internet and rapidly evolving digital communication tools are bringing people everywhere closer together. Children are increasingly conversant with and dependent on these technologies, and the COVID-19 pandemic has accelerated the shift online of many aspects of children's lives.

The internet can be a powerful tool for children to connect, explore, learn, and engage in creative and empowering ways. The importance of the digital environment to children's lives and rights has been emphasised by the United Nations' Committee on the Rights of the Child in General Comment No. 25 adopted in 2021. The General Comment also stresses the fact that spending time online inevitably brings unacceptable risks and threats of harm, some of which children also encounter in other settings and some of which are unique to the online context.

One of the risks is the misuse of the internet and digital technologies for the purpose of child sexual exploitation and abuse. Online grooming, sharing of child sexual abuse material and live-streaming of child abuse are crimes against children that need an urgent, multi-sectoral and global response. These crimes are usually captured in permanent records in the form of digital images or videos, and are perpetually reshared online, victimising children over and over again. As risks of harm continue to evolve and grow exponentially, prevention and protection have become more difficult for governments, public officials and providers of public services to children, but also for parents and caregivers trying to keep-up with their children's use of technology.

With progress being made towards universal internet connectivity worldwide, it is ever -more pressing to invest in children's safety and protection online. Governments around the world are increasingly acknowledging the threat of online child sexual exploitation and abuse, and some countries have taken steps to introduce the necessary legislation and put preventive measures in place. At the same time, the pressure is mounting on the technology industry to put the safety of children at the heart of design and development processes, rather than treating it as an afterthought. This safety-by-design must be informed by evidence on the occurrence of online child sexual exploitation and abuse; *Disrupting Harm* makes a significant contribution to that evidence.

MESSAGE FROM THE END VIOLENCE PARTNERSHIP

The Global Partnership to End Violence against Children, through its Safe Online initiative, invested US$ seven million in the *Disrupting Harm* project. *Disrupting Harm* uses a holistic and innovative methodology and approach to conducting comprehensive assessments of the context, threats and children's perspectives on online child sexual exploitation and abuse. This unprecedented project draws on the research expertise of ECPAT, INTERPOL, UNICEF Office of Research – Innocenti, and their networks. The three global partners were supported by ECPAT member organisations, the INTERPOL National Central Bureaus and the UNICEF Country and Regional Offices. It is intended that this newly developed and tested methodology is applied to additional countries around the world.

Disrupting Harm represents the most comprehensive and large-scale research project ever undertaken on online child sexual exploitation and abuse at a national level and has resulted in 13 country reports and a series of unique 'data insights'. It provides the comprehensive evidence of the risks children face online, how they develop, how they interlink with other forms of violence and what we can do to prevent them.

The findings will serve governments, industry, policy makers, and communities to take the right measures to ensure the internet is safe for children. This includes informing national prevention and response strategies, expanding the reach of *Disrupting Harm* to other countries and regions, and building new data and knowledge partnerships around it.

Disrupting harm to children is everyone's responsibility.

Dr Howard Taylor
Executive Director
End Violence Partnership

EXECUTIVE SUMMARY

Funded by the Global Partnership to End Violence against Children, through its Safe Online initiative, ECPAT International, INTERPOL and UNICEF Office of Research – Innocenti worked in partnership to design and implement a multifaceted research project on online child sexual exploitation and abuse: *Disrupting Harm*. The research was conducted in seven Eastern and Southern African countries and six Southeast Asian countries, including Indonesia. Data are synthesised from up to nine different research activities to generate each national report which tells the story of the threat and presents clear recommendations for action.

Internet access, activities and skills

Ninety-two percent of 12–17-year-olds in Indonesia have used the internet within the past three months. Moreover, according to the *Disrupting Harm* representative household survey of 995 internet-using children in this age group (conducted between November 2020 and February 2021), 95% go online at least once a day. This makes Indonesia a high-connectivity country. Children mainly access the internet from their homes rather than in schools or in internet cafes. Almost all the children surveyed used smartphones to access the internet, and 23% – particularly the younger children – shared these phones with someone else, a lower proportion than in other *Disrupting Harm* countries.

Of those children surveyed, more than nine in ten used the internet for school work at least every week. Other popular online activities included instant messaging (86%) and use of social media (71%). Children's digital skills varied. While 75% claimed that they could determine which images of them or their friends to share online, only 49% knew how to report harmful content on social media, and 58% how to change their privacy settings. Self-reported digital skills were the weakest among children aged 12–13 and children living in rural areas.

One caregiver of each child surveyed was also interviewed. Seventy-two percent of these caregivers were internet-users themselves. When caregivers are confident of their knowledge, they can be useful guides for children's online lives. However, two-thirds of caregivers thought their children knew more about the internet than they did, while only a third were confident of their abilities to check if a website could be trusted or to report harmful content on social media. Internet use and skills were much lower among the older caregivers: up to 64% of caregivers aged 50 and above had never used the internet.

Risky online activities

The great majority of the caregivers surveyed were worried about online risks. They were mostly concerned that their children will talk about sex online or see or send sexual content online. Only 21% of the children – 26% for 12–13-year-olds – said their caregivers restricted their use of the internet. However, 55% of the caregivers said they would do so as a response to their child being bothered by something online.

Most of the children were aware of risks associated with being online. Nevertheless, 11% had, within the past year, met someone in person whom they had first met online (according to the children, many of these encounters were harmless and most of the children were pleased by the experience of meeting someone face-to-face they had got to know first on the internet). Only 1% said that they had shared naked pictures or videos of themselves online – the few that did report this said they did so for fun, because they were in love or flirting, and because they trusted the other person.

Twenty-two percent of the children had come across sexual content unexpectedly online through advertisements, social media feeds, search engines and messaging apps, and 9% reported actively looking for such material. Older children and boys were the most likely to be exposed to sexual images and videos online.

Children's experiences of online sexual exploitation and abuse

The children surveyed were also asked whether they had been subjected to a range of instances of online sexual exploitation and abuse within the past year. Online child sexual exploitation and abuse (OCSEA) refers to situations that involve digital or communication technologies at some point during the continuum of abuse or exploitation. According to *Disrupting Harm* data, in the year prior to being surveyed 2% of internet-using children aged 12–17 in Indonesia were subjected to clear examples of online sexual exploitation and abuse that included blackmailing children to engage in sexual activities, sharing sexual images of without permission, or coercing them to engage in sexual activities through promises of money or gifts. This number likely reflects under-reporting. A minority of the children coerced or blackmailed did what was asked of them. In addition, 2% of children had received unwanted requests to talk about sex and 1% had received requests for images showing their private parts – whether online or offline – from romantic partners, peers, strangers or adults known to them.

In comparison to other Southeast Asian countries where *Disrupting Harm* household surveys were administered, the estimated number of clear instances of OCSEA is low in Indonesia. Moreover, OCSEA may have been under-reported in the household survey due to privacy concerns, shame or discomfort discussing sensitive issues, fear of stigma or self-incrimination, and sampling limitations.

Individuals already known to the child – often adults – were responsible for most instances of OCSEA referred to in the household survey. Individuals previously unknown to the child were involved less frequently. When asked about the most common relationship between offenders and victims in the OCSEA cases they had managed, frontline workers surveyed for *Disrupting Harm* were, in slight contrast to children in the household survey, more likely to say the offenders were strangers, or family friends and community members over 18, in that order.

Meanwhile, the number of reports (known as CyberTips) made to the U.S. National Center for Missing and Exploited Children (NCMEC) by US-based tech companies concerning suspected child sexual exploitation increased by 15% between 2017 and 2019 in Indonesia. The great majority of CyberTips related to the possession, manufacture and distribution of child sexual abuse material (CSAM). There is evidence that CSAM is frequently searched for on the open web and distributed via various channels in Indonesia.

Disclosure and reporting of online sexual exploitation and abuse

Information about the numbers and nature of cases of OCSEA reported, investigated or prosecuted by the law enforcement authorities in Indonesia is limited. Unfortunately, these authorities did not provide *Disrupting Harm* with any data on online and/or offline child sexual abuse and exploitation in Indonesia. Little data is available from the hotlines and helplines.

The household survey of children suggests that OCSEA frequently goes undisclosed and formally unreported. Although 91% of children 'agreed' or 'strongly agreed' that a member of their family would help them if they had a problem, between 17% and 56% (depending on the type of abuse experienced) of the children who were subjected to various forms of OCSEA or other unwanted experiences on the internet did not tell anyone. Those who did so were more likely to confide in a friend or a sibling than in a caregiver or trusted adult. Only one child (who had received unwanted sexual content) reported to the police, and only one child (who had received an offer of money or gifts in exchange for sexual content) called a helpline. Moreover, exceptions to the age of consent and lower penalties apply in the case of rape in the context of marriage.

Reasons given by children for not disclosing OCSEA included: a lack of awareness of where to report or whom to talk to; a sense of having done something wrong; thinking nobody would understand them; concerns about getting into trouble; feelings of shame and embarrassment and concern that it would cause trouble for the family. Data suggests that, while abuse is never a child's fault, children may sometimes be blamed and/or punished for it.

According to criminal justice professionals interviewed, in practice most cases handled by the law enforcement authorities' stem from reports made by adults – sometimes through the helpful mediation of non-government organisations. However, adults too, even if they become aware of OCSEA, may fail to report. Frontline workers and government officials interviewed suggested that lack of awareness of OCSEA as a crime, caregivers' lack of awareness about the risks, and lack of knowledge of reporting mechanisms contributed to non-disclosure and non-reporting. Moreover, more than 80% of the frontline social workers surveyed believed that discomfort around discussing sex and sexuality and the risk of stigma from the community influence the reporting of OCSEA in Indonesia.

Children abused or exploited by offenders of the same sex may have particular difficulty in disclosing OCSEA due to the stigma and penalties surrounding homosexuality in one province, where religious law is upheld, in addition to the Penal Code.

Identification and investigation of OCSEA cases

Some offences relating to OCSEA are defined in the Law on Pornography and in the Penal Code, which contain provisions relevant to CSAM. However, neither law criminalises online sexual extortion or online grooming. Although there are relevant provisions on CSAM in the Law on Pornography, the Penal Code and Law no. 11 of 2008 on Information and Electronic Transactions, which further prohibits any person to distribute, transmit or make accessible "electronic information or electronic documents" containing child sexual abuse, it is not clear if these provisions can be applied to the live-streaming of child sexual abuse, as there is no explicit provision relating to this crime.

The age of sexual consent is set in the Penal Code at 15 years of age for girls. However, conflicting provisions do exist in other pieces of legislation and the relationship between these laws is not clear. There is no minimum age of sexual consent set for boys. An exception for criminal responsibility exists in case of reasonable belief that the girl has reached the age of 15 years. Moreover, exceptions to the age of consent and lower penalties apply in the case of rape in the context of marriage.

The law enforcement mandate to investigate online crimes including OCSEA falls under the Cybercrime Directorate. The Women and Child Protection Unit, which falls under the General Crime Directorate, is responsible for investigating crimes against women and children including child sexual violence, and commonly investigates offline CSEA. For child sexual abuse cases with online components, the unit seeks support from the Cybercrime Directorate which has the necessary tools and expertise to investigate online crimes. The Women and Child Protection Unit has a presence at the national, provincial and district level police units. The Cybercrime Directorate, on the other hand, is at the national level and under which there is a Digital Forensic Unit, which only operates at that national level. At the provincial level, there are 34 Cybercrime sub-directorates. These sub-directorates have no officers within the district level police units, however, when a case involves a child offender or a child victim, the sub-directorates work closely with the Women and Child Protection Unit.

The Digital Forensic Unit reported that it had considerable capacity to address OCSEA, including equipment and tools to undertake investigations (e.g., to triage and analyse CSAM) as well as Standard Operating Procedures for conducting investigations. Despite the availability of equipment, the unit reported having limited human resources. The responding officer has participated in regional and international training programmes provided by foreign law enforcement agencies, including those from the United Kingdom and United States, as well as INTERPOL. Nevertheless, a structured and specialised training programme on victim identification was stated by the law enforcement agencies as an unmet need.

This could be an indicator of frequent transfers of officers to other roles with different job descriptions and of the lack of a defined mechanism for institutional knowledge management. There are no Standard Operating Procedures for inter-ministerial coordination between the national law enforcement authorities and the Ministry of Communication and Information Technology for sharing data on OCSEA. There is no national system to manage sex offenders.

Children's experiences with law enforcement mechanisms, the justice process and social services

During the course of the data collection for *Disrupting Harm*, the research team was unable to identify child victims of OCSEA who had sought justice through the courts in order to interview them, for the most part due to COVID-19 lockdown and travel restrictions. Consequently, the following information on what happens when cases of OCSEA come to the attention of the authorities relies solely on the interviews and surveys with government officials, justice officials and frontline service providers, thus potentially missing out on critical information from children themselves.

When interviewing child victims, it is reported that trained officers from the Women and Child Protection Unit are involved in the interviews, which take place in special interview rooms (sometimes through cooperation with non-governmental organisations), and that the officers are in civilian clothes, rather than in uniform. However, such child-friendly arrangements are not available across police stations at the district, city and provincial level. Another challenge that emerged in relation to the implementation of child-friendly measures by the police is the frequent transfer of officers trained in child-friendly measures to other duties, and this may hamper the effectiveness of any training programmes undertaken for law enforcement officers. It also emerged that the number of police officers specialising in children's cases is limited when compared to the number of children's cases. Staffing capacity was said to constitute a challenge not only in the police force but also among prosecutors and judges with respect to the specialised knowledge necessary to handle children's cases.

Government representatives and criminal justice professionals pointed out that some reports of OCSEA do not culminate in the prosecution of the offender. In some cases, the children or their caregivers were said to withdraw their complaints due to intimidation by offenders, or as a result of pressure from families and communities. In other cases, digital evidence could not be secured.

Court proceedings are reportedly conducted in juvenile courtrooms closed to the public, judges wear normal civilian clothing, and efforts are made to protect the victims' identities. However, these measures may not be implemented in remote regions outside of the major cities. Some criminal justice professionals were said to not always use child-friendly approaches when interacting with child victims. Due to the limitation in the number of criminal justice professionals specialising in children's cases, cases can become drawn-out due to the time required to collect evidence, adding to the trauma of the victims and their families.

The Child Protection Law requires that a child victim be provided with protection and be accompanied by caregivers or social workers during the criminal justice process. The right to legal assistance is not specified in the Child Protection Law for child victims. On 12th April 2022, the Indonesian parliament approved the Sexual Violence Bill but, as the signed and final version of this law was not publicly available during the writing of this report, the research team could not establish if the right to legal assistance for victims of child sexual abuse and exploitation is explicitly covered in this law. There are however non-governmental organisations which provide legal assistance to child victims. The law also provides for the restitution of damages, but victims are often unaware of this, and prosecutors may not apply for it. In addition, enforcing restitution orders is a major challenge as offenders may opt for longer prison sentences instead of paying the restitution directed by the court order.

The survey of frontline service providers suggested that medical and psychosocial support services for victims are generally good but are not made available in every case. In this context, the Women and Child Protection Unit cooperates with the Unit *Pelaksana Teknis Daerah Perlindungan Perempuan dan Anak*, (UPTD PPA) and the Integrated Service Centres for the Empowerment of Women and Children (*Pusat Pelayanan Terpadu Perlindungan Perempuan dan Anak* – P2TP2As), which act as referral centres and coordinate with other service providers in providing support services to child victims of violence. Although they have been established by the government, the P2TP2As depend on support from volunteers and civil society, whereas UPTD PPAs have human resources, though these are also limited. The lack of resources and capacity for child protection at the district level hinders the UPTD PPAs and P2TP2As from effectively executing their mandate.

Current initiatives for children

In 2019, Indonesia adopted the Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN, thereby committing itself to improving child protection standards and policies on OCSEA, enhancing the capabilities of professionals, establishing a unit specialised in investigating OCSEA-related crimes, strengthening data collection mechanisms, raising awareness and engaging with the private sector. In September 2021, Indonesia adhered to the earlier ASEAN Regional Plan of Action on the Elimination of Violence against Children 2016-2025, which commits the country to developing preventive measures and amending laws against OCSEA.

Despite these commitments, and a willingness to acknowledge that OCSEA is a rising threat, some government representatives noted that the government's current efforts to address OCSEA are limited. Coordination, awareness, capacity, funding and data collection regarding OCSEA were specifically mentioned by interviewees as areas that could be improved.

The drafting of a Child Protection Online Road Map was initiated by the Ministry of Communication and Information Technology in 2017 and aims to guide stakeholders – including government, law enforcement agencies, the industry, civil society and community members – as to the actions they should take to promote access to a safer internet for children. The government intends to finalise and adopt the Road Map as a presidential decree that will be binding to relevant mandated government agencies. As of June 2022, the Road Map was yet to be finalised and formally adopted.

Indonesian law does not contain any provisions that explicitly compel Internet service providers to filter and/or block child sexual abuse material and report companies and/or individuals disseminating, trading, or distributing these materials. On the other hand, local Internet service providers are obliged to block negative content including 'pornography' and to share information with law enforcement agencies. The Ministry of Communication and Information Technology maintains a database of websites that must be blocked. It also operates a Negative Content Crawling Machine which helps to detect broadly inappropriate content and block it from spreading further.

The Ministry of Communication and Information Technology and the Ministry of Women's Empowerment and Child Protection are seen as the main institutions with a mandate for combating OCSEA, together with the Ministry of Social Affairs. There is an inter-agency Task Force for Anti-Pornography, but it is not clear from this research how active it is in the coordination of responses to OCSEA.

Civil society organisations are active in the provision of services such as assisting victims and caregivers when they report OCSEA to law enforcement units, and in providing legal aid and psychosocial support.

Key insights

This report concludes by highlighting six key insights from the research:

1. In the past year, at least 2% of internet-using children aged 12–17 in Indonesia were subjected to clear examples of online sexual exploitation and abuse that included being blackmailed to engage in sexual activities, having their sexual images shared without permission, or being coerced to engage in sexual activities through promises of money or gifts. This number likely reflects underreporting.

2. According to the household survey, OCSEA offenders are most often people already known to the child – often an adult friend, a peer or a family member.

3. Children who were subjected to OCSEA on social media mainly said this happened through major platforms such as WhatsApp, Facebook and Facebook Messenger.

4. Children who were subjected to OCSEA tended to confide in people within their interpersonal networks, particularly their friends and siblings. Helplines and the police were almost never avenues they sought help.

5. The mandated government agencies in Indonesia acknowledge that OCSEA is a threat, but government efforts to address it need to be more extensive. The capacities of law enforcement agencies, justice professionals and social support workers to provide victims of OCSEA with access to child-friendly justice and support services is limited by the low levels of awareness of OCSEA, insufficient human and budgetary resources, and inadequate technical knowledge and skills.

6. Although existing legislation, policies and standards in Indonesia include provisions relevant to OCSEA, further legislative action is needed to criminalise all OCSEA-related acts.

The report ends with a detailed road map to be used by all relevant stakeholders in protecting children from online sexual exploitation and abuse: government; law enforcement; justice and social services sectors and those working within them; communities, teachers and caregivers; and digital platforms and service providers. Many of the recommendations align with the 2021 Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN. The recommendations are too detailed to be recounted in the Executive Summary but can be found in full on page 91 of this report.

DISRUPTING HARM METHODS

As with all the settings in which children live and grow up, the online environment may expose them to risks of sexual exploitation and abuse. Yet the scarcity of the available evidence makes it difficult to grasp the nature of the harm caused, or to make constructive recommendations on public policies for prevention and response. Informed by the 2018 WeProtect Global Alliance Threat Assessment[1] and a desire to understand and deepen the impact of its existing investments, the Global Partnership to End Violence against Children, through its Safe Online initiative, decided to invest in research to strengthen the evidence base on online child sexual exploitation and abuse (OCSEA) – with a particular focus on 13 countries across Eastern and Southern Africa and Southeast Asia.

Figure 1: *Disrupting Harm* methods in Indonesia.

PHASE 2

Survivor conversations n = 0

Household survey data from children and parents n = 995

Government duty-bearer interviews n = 12

Frontline service providers' survey n = 50

Access to justice interviews with professionals n = 10

Access to justice interviews with children n = 0

Non-law enforcement data analysis

Law enforcement capacity assessment n = 1

Country threat assessment n = 0

PHASE 1

Desk review of relevant documents

Legal analysis

1. WeProtect Global Alliance (2018). Global Threat Assessment 2018: Working together to end the sexual exploitation of children online. London: WeProtect Global Alliance.

The countries of focus in the Eastern and Southern Africa region are Ethiopia, Kenya, Mozambique, Namibia, South Africa, Tanzania, and Uganda. The countries of focus in the Southeast Asian region are Cambodia, Indonesia, Malaysia, the Philippines, Thailand, and Vietnam.

ECPAT, INTERPOL and UNICEF Office of Research – Innocenti worked in collaboration to design and implement the *Disrupting Harm* project. In total, the three organisations collected data for six unique research activities. Extensive data collection took place in Indonesia from early 2020 through to early 2021. This process took place during the COVID-19 pandemic, as a result of which Indonesia experienced a lockdown as one of the measures to curb the pandemic, which may have influenced the data. During an extensive analysis phase the data from all the research activities were triangulated and a series of 13 country reports were developed. The analysis for Indonesia was finalised in January 2022. Using the same methodology in all 13 countries also allows for comparisons between countries.

Aside from its sheer scope and its facilitation of comparisons between countries, the project is also unique as it brings together the specific and complementary expertise of three global networks, ECPAT, INTERPOL and UNICEF.

The desired outcome of this report is to provide a baseline and evidence for Indonesian policy makers to tackle and prevent OCSEA, and to strengthen support for children. In addition, the findings and recommended actions are expected to have relevance for a broader global audience. The recommended actions proposed in the report are aligned with the WeProtect Model National Response[2] and contribute to the 2030 Agenda for Sustainable Development.[3]

Summary of methods used by ECPAT in Indonesia

Interviews with government representatives

Between May 2020 and August 2020, 11 semi-structured interviews were conducted with a total of 12 senior national government representatives holding specific responsibilities to respond to the risks of OCSEA at a national level.[4] Due to the COVID-19 pandemic, some interviews were conducted in person and others virtually. More information on the methodology can be found here, while the preliminary report of this data can be found here. Attributions to data from these respondents have ID numbers beginning with RA1 throughout the report.[5]

Analysis of non-law enforcement data and consultations

A range of non-law enforcement stakeholders have data and insights on the nature and scale of OCSEA. Data were obtained from the International Association of Internet Hotlines (INHOPE), the Internet Watch Foundation and Child Helpline International. Qualitative insight was provided by a number of global technology platforms. Where relevant, this information supplements the analysis contributed by INTERPOL.

Survey of frontline social support workers

A non-probability convenience sample of 50 client-facing frontline workers in Indonesia, including outreach youth workers, social workers, case managers, psychologists and health and legal professionals directly working with children's cases, participated in a survey administered online between March and August 2020.

---

2. WeProtect Global Alliance. (2016). Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response. London: WeProtect Global Alliance.
3. See goals 5.2, 8.7 and 16.2 in the resolution adopted by the UN General Assembly (A/RES/70/1) 70/1. Transforming our world: the 2030 Agenda for Sustainable Development.
4. The senior national government representatives were from the following government departments and ministries: the Cybercrime Unit of the Indonesia National Police; Women and Child Protection, Indonesia Police Department; Ministry of Women Empowerment and Child Protection; Ministry of Law and Human Rights; Ministry of National Development Planning of the Republic of Indonesia; Attorney General's Office; Indonesian Child Protection Commission; Ministry of Communication and Information Technology; Ministry of Social Affairs, and the National Cyber and Crypto Agency.
5. The format RA1-IN-01-A is used for IDs. 'RA1' indicates the research activity, 'IN' denotes Indonesia, '01' is the participant number and 'A' indicates the participant when interviews included more than one person.

This research activity aimed to explore the scope and context of OCSEA as it is observed by those working on the social support front line to prevent and respond to it. More information on the methodology can be found here, while the preliminary summary report of this data can be found here. Attributions to data from these respondents have ID numbers beginning with RA3 throughout the report.

Access to Justice interviews with OCSEA victims and their caregivers

This activity was not undertaken in Indonesia. The high rates of COVID-19 infection at the time of data collection resulted to a prolonged period of lockdown and travel restrictions. This hindered the identification of OCSEA victims, as it was not possible for the consultant assigned to this task to organise meetings with individuals and organisations that would have assisted in the identification of OCSEA victims and caregivers to be interviewed. In addition, unlike the other activities that could be conducted virtually, interviews with OCSEA victims and caregivers had to be conducted face-to-face and, with the lockdown and travel restrictions in place, this was not possible. It was for these reasons that this activity was suspended in Indonesia. The perspectives of OCSEA victims and their caregivers are therefore unfortunately not represented in the Indonesia report. More information on the methods of this research activity (conducted in countries where a sample was identified) can be found here.

Access to Justice interviews with justice professionals

Ten semi-structured interviews were conducted with ten criminal justice professionals in July and August 2020. The sample included government and non-government respondents who had experience with OCSEA criminal cases.[6] More information on the methodology can be found here, while the preliminary summary report of the data can be found here. Attributions to data from these respondents have ID numbers beginning with RA4 throughout the report. The suffix 'justice' is also included in the ID numbers for clarity.

Literature review and legal analysis

A literature review was undertaken to inform the research teams prior to the primary data collection. This comprehensive analysis of the legislation, policy and systems addressing OCSEA in Indonesia was conducted and finalised in May 2020. More information on the methodology can be found here, while the full report on the legal analysis can be found here.

Conversations with OCSEA survivors

Unstructured, one-on-one conversations led by trauma-informed expert practitioners were arranged with 33 young survivors of OCSEA in five selected *Disrupting Harm* countries (nine girls in Kenya; five boys and seven girls in Cambodia; seven girls in Namibia; four girls in Malaysia, and one boy in South Africa). Although not held in all countries, these conversations are meant to underline common themes and issues in all 13 *Disrupting Harm* countries. More information on the methodology can be found here. The report presenting the analysis of all 33 survivor conversations from five *Disrupting Harm* countries will be published in 2022. Attributions to data from these respondents have ID numbers beginning with RA5 throughout the report.

Summary of methods used in Indonesia by INTERPOL

Quantitative case data analysis

Data on cases related to OCSEA was requested from law enforcement authorities via the INTERPOL National Central Bureau in each country. Data were also obtained from the mandated reports of United States-based technology companies to the National Center for Missing and Exploited Children (NCMEC) and from a number of other partner organisations with a view to deepening the understanding of relevant offences committed in the country, offender and victim behaviour, crime enablers and vulnerabilities. Indonesia national law enforcement did not share any qualitative and quantitative data on crime statistics pertaining to country threat.

---

6. The following state and non-state agencies were represented in the interviews: Technical Implementation Unit; the Integrated Service Centre for the Empowerment of Women and Child (P2TP2A) DKI Jakarta; Surabaya Children Crisis Centre; Witness and Victim Protection Agency; Bahtera Foundation; Embun Pelangi Foundation
Centre for Study and Child Protection; Anti-Human Trafficking National Network; Social Service; Don't Be Naked in front of The Camera Movement, and the Supreme Court.

Qualitative capacity assessments

In addition to seeking data on OCSEA cases, INTERPOL requested data on the capacity of the national law enforcement authorities to respond to this type of crime, and interviewed one serving officer. Particular emphasis was placed on human resources, access to specialist equipment and training, investigative procedures, the use of tools for international cooperation, and to achievements and challenges. Attributions to data from this activity have ID numbers beginning with RA8 throughout the report.

More information on INTERPOL's methodologies can be found here.

Summary of methods used in Indonesia by UNICEF Office of Research – Innocenti

Household survey of internet-using children and their caregivers

In order to understand children's use of the internet, the risks and opportunities they face online, and the risk of OCSEA in particular, a nationally representative household survey was conducted with 995 internet-using children. The term 'household survey' is used throughout the report to indicate findings that come from this specific research activity. The target population for the survey was children aged 12–17 in Indonesia who had used the internet in the three months before the interview. Additionally, one parent or caregiver of each child was interviewed. The term 'household survey' is used throughout the report when referring to the findings from this research activity. The survey sample was composed of 451 (45%) boys and 544 (55%) girls. Of these children, 295 (30%) were 12–13-year-olds, 342 (34%) were 14–15-year-olds and 358 (36%) were 16–17-year-olds.

To achieve a nationally representative random sample, the survey used random probability sampling with national coverage. Coverage is defined as the proportion of the total population that had a chance of being included in the survey sample – meaning that the fieldwork would cover the area where they live if sampled.

In Indonesia, Primary Sampling Units were selected using a two-stage design. Given the large variation of province sizes in Indonesia, the thirteen largest provinces were purposively selected (based on population size and accessibility), and others were excluded. Given the dispersed geography of the country, for logistical and cost efficiencies, the following provinces were excluded from the frame: Aceh, Bali, Bengkulu, Daerah Istimewa Yogyakarta, Gorontalo, Jambi, Kalimantan Selatan, Kalimantan Tengah, Kalimantan Utara, Kepulauan Bangka Belitung, Kepulauan Riau, Maluku Utara, Nusa Tenggara Barat, Nusa Tenggara Timur, Papua Barat, Riau, Sulawesi Barat, Sulawesi Tengah, Sulawesi Tenggara, Sumatra Barat and Sumatra Utara. This approach resulted in 76% fieldwork coverage. However, the survey sample covered almost all the main regions, including Java, Kalimantan, Maluku, Papua, Sulawesi and Sumatra. Despite the exclusions, the data is still expected to represent a strong indication of the issues explored.

The sampling followed a multi-stage random probability clustered sample design. Within the 13 provinces selected, a total of 20 districts were sampled. First, the number of districts to select in each province was allocated, ensuring at least one district was allocated to every covered province and otherwise allocating in proportion to the population sizes at the province level. Within each province, the number of districts selected was allocated according to Probability Proportional to Size. The next step was to select Primary Sampling Units in each district. To achieve the required 100 Primary Sampling Units for data collection, a fixed number of Primary Sampling Units to be sampled per district was determined. The fixed number was set so the total number of Primary Sampling Units sampled per province was as close to the population distribution as possible. The specified number of Primary Sampling Units were then randomly sampled from each district, following Probability Proportional to Size. The Primary Sampling Units list was taken from the Indonesia 2010 Population Census which was provided by Statistics Indonesia (*Badan Pusat Statistik*).

Within each primary sampling unit, interviewers selected addresses in the field using random walk procedures and attempted contact at the selected addresses to screen for members of the survey population using a screening question developed for this purpose. Finally, individuals (children and caregivers) were selected within each eligible household using random methods.

In every household visited *Disrupting Harm* attempted to collect data on the number of 12–17-year-old children in the household, their gender, and whether they had used the internet in the past three months. This allowed *Disrupting Harm* to estimate internet penetration rates for all 12–17-year-olds in Indonesia.

The fieldwork took place between 26 November 2020 and 28 February 2021. Data collection was coordinated by Ipsos MORI and carried out by Ipsos Indonesia on behalf of UNICEF Office of Research – Innocenti.

To enhance the precision of the estimates presented, the household survey data used throughout this report was weighted following best practice approaches for the weighting of random probability samples. The weighting included the following stages:

- Design weight adjustments to reflect the probabilities of selection (inverse probability weights);

- Non-response weights to reduce non-response bias; and

- Post-stratification weights to adjust for differences between the sample and population distributions.

A more detailed explanation of the methodological approach and the specific methods used for analysis of the household survey data can be found here.

Ethical Approval

The UNICEF Innocenti research component received ethical approval from the Health Research Ethics Committee, National Institute of Health Research and Development. ECPAT International's research components received approvals from the LIPI Lembaga Ilmu Pengetahuan Indonesia (Indonesian Institute of Sciences) Ethical Review Board at a national level. The protocols of ECPAT and UNICEF were also reviewed and approved by the Health Media Lab Institutional Review Board.

INTERPOL assessed the threat of OCSEA and the capacity of the law enforcement authorities to counter it. These assessments entailed interviews with law enforcement officers in units dealing with the crime area and with staff of police units and national agencies that handle police data. INTERPOL did not have contact with children or victims. Nevertheless, to ensure proper ethical conduct and research standards, the INTERPOL team completed an online course on Responsible Conduct of Research from the Collaborative Institutional training Initiative and followed the INTERPOL Code of Conduct.

National Consultation

In a national consultation that took place on March 17, 2022, representatives of the government, law enforcement authorities and civil society in Indonesia were asked to provide input on the *Disrupting Harm* findings and recommended actions to enhance their relevance for the Indonesian context.

ABOUT ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

Child sexual abuse **refers to various sexual activities perpetrated on children (persons under 18), regardless of whether or not the children are aware that what is happening to them is neither normal nor acceptable. It can be committed by adults or peers and usually involves an individual or group taking advantage of an imbalance of power. It can be committed without explicit force, with offenders frequently using authority, power, manipulation or deception.[7]**

Child sexual exploitation involves the same abusive actions. However, an additional element of a threat or of exchange for something (e.g., money, material goods, immaterial things like protection or shelter, a relationship, or even the mere promise of such) must also be present.[8]

> ***Online child sexual exploitation and abuse (OCSEA)*** refers to situations involving *digital, internet* and *communication technologies* at some point during the continuum of abuse or exploitation. OCSEA can occur fully online or through a mix of online and in-person interactions between offenders and children.

Disrupting Harm also focuses on how technology can be misused to facilitate child sexual exploitation and abuse. Its use of the term 'OCSEA' does not refer to abuse or exploitation that occurs exclusively online, nor is it the intention of *Disrupting Harm* to create an artificial divide between online and offline child sexual exploitation and abuse. Children can be abused or exploited while they spend time in the digital environment, but equally, offenders can use digital technologies to facilitate their actions – e.g., to document and share images of in-person abuse and exploitation or to groom children to meet them in person.

Any characterisation of OCSEA must recognise that the boundaries between online and offline behaviour and actions are increasingly blurred[9] and that responses need to consider the whole spectrum of activities in which digital technologies may play a part. This characterisation is particularly important to keep in mind as children increasingly see their online and offline worlds as entwined and simultaneous.[10]

For *Disrupting Harm*, OCSEA was defined specifically to include child sexual exploitation and abuse that involves:

- Production, possession or sharing of **child sexual abuse material (CSAM):** Photos, videos, audios or other recordings, or any other representation of real or digitally generated child sexual abuse or sexual parts of a child for primarily sexual purposes.[11]

- **Live-streaming of child sexual abuse:** Child sexual abuse that is perpetrated and viewed simultaneously in real-time via communication tools, video conferencing tools and/or chat applications. In most cases, the offender requesting the abuse in exchange for payment or other material benefits is physically in a different location from the child(ren) and the facilitators of the abuse. **Online grooming of children for sexual purposes:** Engagement with a child via technology with the intent of sexually abusing or exploiting the child.

---

7. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 18.

8. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 24.

9. May-Chahal, C., Palmer, E., Dodds, S., & Milan, S. (2018). Rapid Evidence Assessment: Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation. UK: Lancaster University.

10. Stoilova, M., Livingstone, S., and Khazbak, R. (2021). Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes. Innocenti Discussion Paper 2020-03. UNICEF Office of Research – Innocenti.
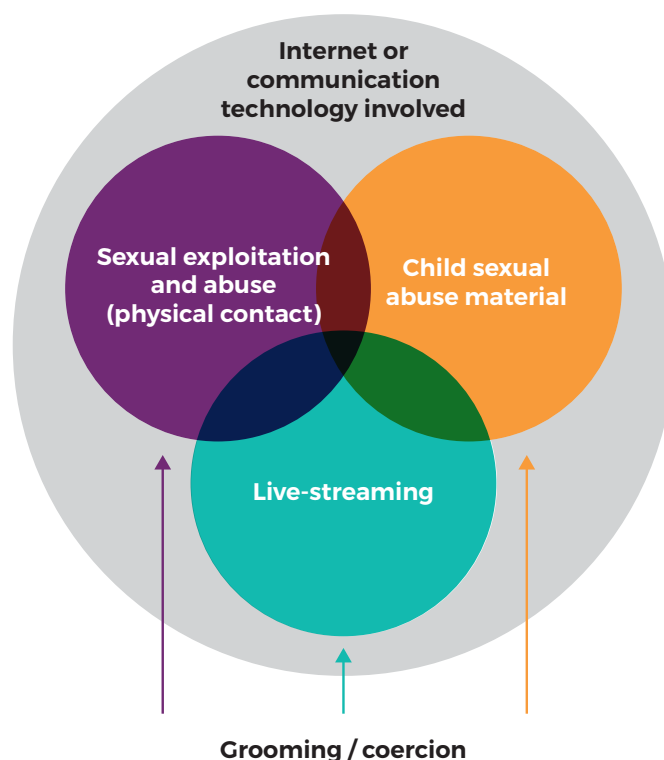
11. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 40.

Figure 2: Framing the main forms of online child sexual exploitation and abuse explored by *Disrupting Harm*.

Internet or communication technology involved

Sexual exploitation and abuse (physical contact)

Child sexual abuse material

Live-streaming

Grooming / coercion

While international legal instruments[12] criminalising grooming indicate that this must take place with intent to meet the child in person, it has become increasingly common for offenders to sexually abuse children by, for example, manipulating them into self-generating and sharing CSAM through digital technologies, without necessarily having the intention of meeting them and abusing them in person.

The *Disrupting Harm* reports also address other phenomena that contribute to understanding the contexts and socio-cultural environments in which OCSEA occurs.

- **The sharing of self-generated sexual content involving children**[13] can lead to or be part of OCSEA, even if this content is initially produced and shared voluntarily between peers, as it can be passed on without permission or obtained through deception or coercion.

- **Sexual extortion of children**[14] refers to the use of blackmail or threats to extract sexual content or other benefits (e.g., money) from the child, often using sexual content of the child that has previously been obtained as leverage.

- **Sexual harassment of a child**[15] and **unwanted exposure of a child to sexual content**[16] are other phenomena which *can* constitute or enable OCSEA in some instances. For example, offenders can deliberately expose children to sexual content as part of grooming to desensitise them to sexual acts. However, for the purpose of evidence-based policy and programme development, it is important to acknowledge that there are differences between voluntary viewing of sexual content by children and viewing that is forced or coerced. The former is not included in the definition of OCSEA adopted for *Disrupting Harm*.

12. The only two legally binding international instruments containing an obligation to criminalise the grooming of children for sexual purposes are: Council of Europe. (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Council of Europe Treaty Series – No. 201, Article 23; and European Parliament and Council. (2011). Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Article 6.
13. Cooper, K., Quayle, E., Jonsson, L., & Svedin, C.G. (2016). Adolescents and self-taken sexual images: A review of the literature. *Computers in Human Behavior*, *55*, 706-716.
14. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 52.
15. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 21.
16. Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 44.

ABOUT INDONESIA – DEMOGRAPHICS AND INTERNET USAGE

Despite increasing connectivity around the world, few countries regularly update their formal internet use statistics or disaggregate them for their child populations. This presents a challenge in understanding how young people's lives are impacted by digital technologies, particularly in low- and middle-income countries. The infographic below summarises the latest data on internet access and social media use in Indonesia, some of which was gathered directly through the *Disrupting Harm* nationally representative household survey of internet-using 12–17-year-olds.

The data presented here provide an important backdrop for understanding the various facets of children's internet use. However, methodological limitations may affect the quality of data from some secondary sources. Reliance on purposive or other non-probability sampling techniques means that the data cannot be considered representative of the population in question. In addition, variations in data collection methods and definitions of internet use pose a challenge for comparisons between the different countries.

POPULATION TOTAL 2020
Country data:
269,603,400[17]
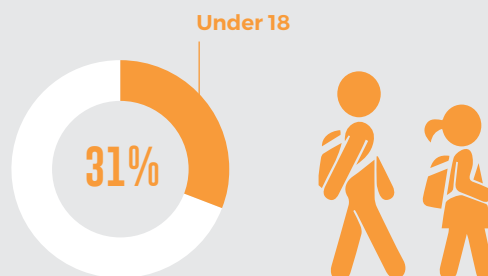
FEMALE POPULATION 2020
Country data:
134,266,400[18]

MALE POPULATION 2020
Country data:
135,337,000[19]

POPULATION UNDER 18 2020
UN data:
84,934,000

Under 18

31%

URBAN POPULATION 2018: 55%[20]
2030 prospective: 63%[21]

Urban

55%
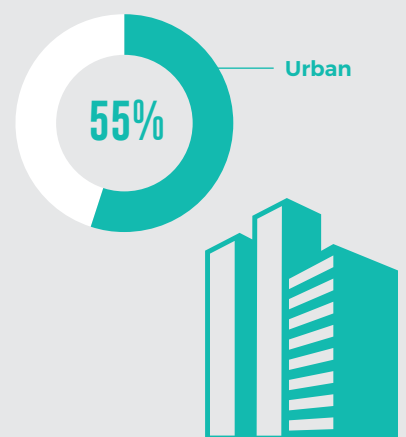
MEDIAN AGE 2020
30[22]
Estimate

GDP PER CAPITA 2019 (US$)
$3,870[23]

17. Badan Pusat Statistik (BPS - Statistics Indonesia) (n.d.) Total Population Projection Result by Province and Gender (Thousand People), 2018-2020.
18. Badan Pusat Statistik (BPS - Statistics Indonesia) (n.d.) Total Population Projection Result by Province and Gender (Thousand People), 2018-2020.
19. Badan Pusat Statistik (BPS - Statistics Indonesia) (n.d.) Total Population Projection Result by Province and Gender (Thousand People), 2018-2020.
20. United Nations Population Division. (2018). World Population Prospects 2019 File 1: Population of Urban and Rural Areas at Mid-Year (thousands) and Percentage Urban, 2018.
21. United Nations Population Division. (2018). World Population Prospects 2019 File 1: Population of Urban and Rural Areas at Mid-Year (thousands) and Percentage Urban, 2018.
22. United Nations Population Division. (2019). World Population Prospects 2019 File POP/5: Median age by region, subregion and country, 1950-2100 (years).
23. The World Bank. (n.d.) GDP per capita (current US$) - Indonesia.

ABOUT INDONESIA – DEMOGRAPHICS AND INTERNET USAGE

POVERTY RATES

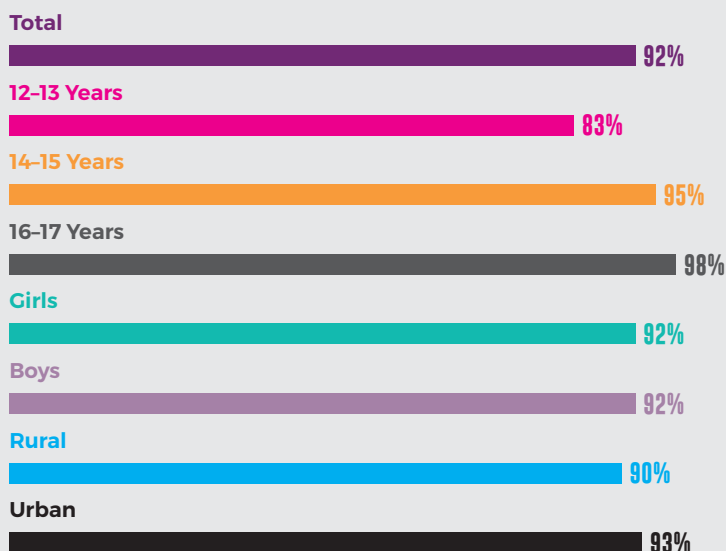Poverty headcount ratio at national poverty lines (% of population)[24]

9%

LANGUAGE

INDONESIAN

THE OFFICIAL LANGUAGE IS INDONESIAN (BAHASA INDONESIA)[25]

Source: Disrupting Harm data

2020 INTERNET PENETRATION RATES AMONG 12–17-YEAR-OLDS

Total	92%
12–13 Years	83%
14–15 Years	95%
16–17 Years	98%
Girls	92%
Boys	92%
Rural	90%
Urban	93%

n = 1,490 households.

Source: Disrupting Harm data

INTERNET USE AMONG CAREGIVERS OF INTERNET-USING CHILDREN
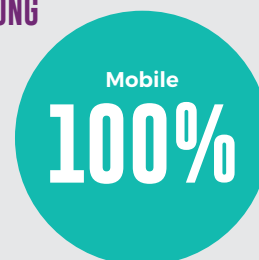
72%

n = 995 caregivers of internet-using children.

INTERNET SUBSCRIPTION/ PENETRATION RATES 2019: 48%[26]

48%

Source: Disrupting Harm data

MOST POPULAR DEVICE TO ACCESS THE INTERNET AMONG 12–17-YEAR-OLDS*

- **0.2% Tablet**
- **6% Computer**
- **Mobile 100%**

n = 995 internet-using children.

*Multiple choice question

Source: Disrupting Harm data

MOST POPULAR PLACE TO ACCESS THE INTERNET AMONG 12–17-YEAR-OLDS*

- **Internet café** 20%
- **Mall** 27%
- **School** 62%
- **Other** 78%
- **Home** 100%
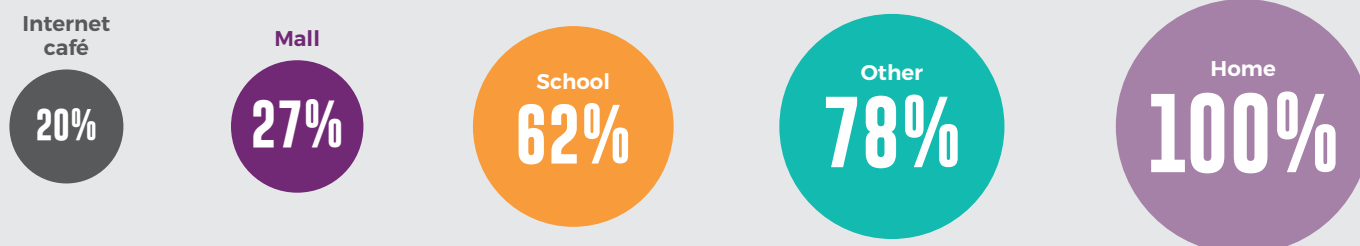
n = 995 internet-using children.   *Multiple choice question

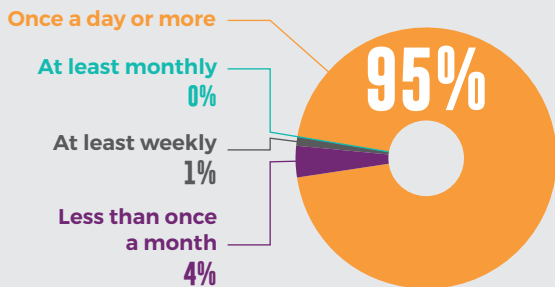24. World Bank. (n.d.). Poverty & Equity Data Portal.
25. Government of Indonesia (1945). Constitution of the Republic of Indonesia, Article 36.
26. Badan Pusat Statistik (BPS - Statistics Indonesia) (n.d.) Proportion of Individuals Who Use the Internet by Province (Percent), 2017-2019.
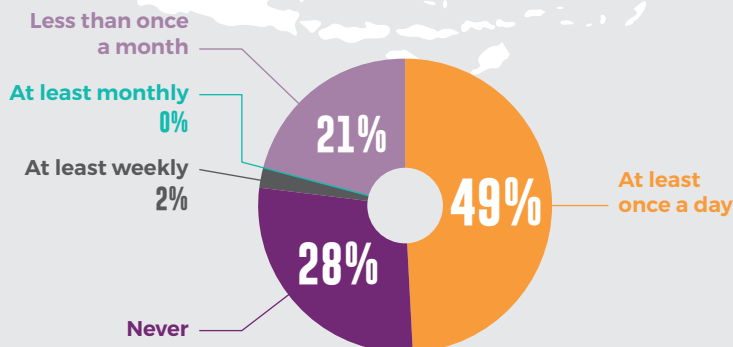
ABOUT INDONESIA – DEMOGRAPHICS AND INTERNET USAGE

FREQUENCY OF INTERNET USE AMONG 12–17-YEAR-OLDS

Once a day or more

At least monthly
0%

At least weekly
1%

Less than once
a month
4%

95%

n = 995 caregivers of internet-using children.

FREQUENCY OF INTERNET USE AMONG CAREGIVERS OF INTERNET-USING CHILDREN

Less than once
a month

At least monthly
0%

At least weekly
2%

21%

49% At least once a day

28%

Never

n = 995 caregivers of internet-using children.

CHILDREN WHO USE SOCIAL MEDIA ON A WEEKLY BASIS

Total	12-13	14-15	16-17	Boys	Girls
71%	63%	70%	78%	68%	73%

n = 995 internet-using children.

CHILDREN WHO USE INSTANT MESSAGING APPS ON A WEEKLY BASIS

Total	12-13	14-15	16-17	Boys	Girls
86%	79%	86%	92%	85%	87%

n = 995 internet-using children.

ICT DEVELOPMENT INDEX RANKING (ITU) 2017

Asia & Pacific 19/34[27]

World 111/176
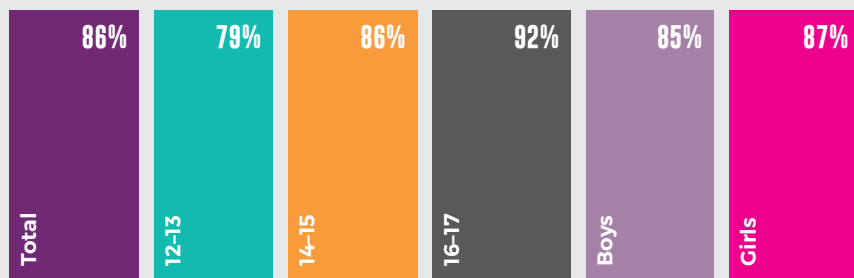
GLOBAL CYBERSECURITY INDEX RANKING 2018[28]

Asia & Pacific 9/38[29]

World 41/175

---

27. International Telecommunication Union. (2017). ICT Development Index 2017. (Note: a higher ranking indicates better ICT development)
28. The Global Cybersecurity Index measures the commitment of countries to cybersecurity based on the implementation of legal instruments and the level of technical and organisational measures taken to reinforce international cooperation and cybersecurity.
29. International Telecommunication Union. (2019). Global Cybersecurity Index (GCI) 2018.

OVERVIEW OF LEGISLATION AND POLICY

Some offences relating to OCSEA have been addressed through the Law No. 44 of 2008 on Pornography.[30] In addition, the Penal Code[31] contains provisions relevant to child sexual abuse material (CSAM).

The Law on Pornography defines CSAM as "all kinds of pornography that involve a child or include an adult who acts like a child."[32] As this law prohibits conduct related to pornography in general[33] (i.e., including materials depicting adults), this prohibition also applies to CSAM as this is considered a type of pornography in light of the definition above. Pornography-related offences, including viewing,[34] carry penalties of up to 12 years of imprisonment and/or fines of up to six billion Indonesian Rupiah (approximately USD 405 in June 2022, exact penalties depend on the offence).[35] In the case of CSAM, penalties are increased by one third.[36]

The Penal Code criminalises conduct related to writings, portraits or objects offensive to decency.[37] The vague wording of the provision leaves the possibility of invoking this provision for CSAM-related crimes open to judicial interpretation. The Penal Code also criminalises the public exhibition or display of writings or portraits that "arouse or stimulate the sensuality" of children under 17 years of age.[38]

Crucially, neither the Law on Pornography nor the Penal Code criminalises online sexual extortion, online sexual harassment or the live-streaming of child sexual abuse. The Law on Pornography does contain a provision referring to pornographic performances and prohibiting any person from "showing themselves or other people in performances or in front of public that describes nakedness, sexual exploitation, sexual intercourse, or other that contains pornography elements".[39] However, it is not specified whether this could cover live-streaming of child sexual abuse.

In April 2022, the new Sexual Violence Bill was approved. Although the latest draft of the bill is not publicly available at the time of finalisation of this report, insights received during the drafting of this report, indicate that the bill includes a definition of sexual exploitation and sexual harassment – although not specific to crimes committed in the online environment.

With respect to provisions of law on sexual exploitation which are also relevant to OCSEA-related crimes, it is worth mentioning that the Penal Code sets the age of sexual consent at 15 years, though only for girls and outside of marriage.[40] However, conflicting provisions do exist in other pieces of legislation and the relationship between these laws is not clear.[41] A further provision criminalises adults who commit "obscene acts" with a minor of the same sex,[42] which implicitly sets the age of consent for homosexual sex at 18. However, for boys there is no age of consent established for heterosexual sex.

30. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography.
31. Government of Indonesia (1999). Penal Code of the Republic of Indonesia.
32. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Elucidation of Section 4(1)(f).
33. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Sections 4, 5 and 6.
34. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Section 6.
35. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Chapter VII.
36. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Section 37.
37. Government of Indonesia (1999). Penal Code of the Republic of Indonesia, Article 282 (2).
38. Government of Indonesia (1999). Penal Code of the Republic of Indonesia, Article 533.
39. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Article 10.
40. Government of Indonesia (1999). Penal Code of the Republic of Indonesia, Section 287.
41. UNICEF. (2015). Legal Protection from Violence: Analysis of domestic laws related to violence against children in ASEAN member States. UNICEF EAPRO: Bangkok. citing Government of Indonesia (2002). Child Protection Law (as amended in 2014) (Untranslated), Article 18.
42. Government of Indonesia (1999). Penal Code of the Republic of Indonesia, Section 292.

This failure to set a minimum age for boys excludes them from being considered victims of statutory rape. In addition, exceptions to the age of sexual consent exist in relation to the rape of girls in the context of marriage.[43] As reported by media, the newly approved Sexual Violence Bill would fill this gap by recognising boys as victims of rape and marital rape.[44,45] In one province, where religious law additional to the Penal Code is upheld, Muslim males and females can be penalised for sex outside of marriage or for sex between same-sex partners.[46]

In terms of the extraterritorial applicability of Indonesian law, the Penal Code establishes jurisdiction over any offence or illegal conduct committed abroad by an Indonesian national, as long as it is also considered a crime in the country where it occurs (double criminality principle).[47] National legislation does not explicitly recognise extraterritorial jurisdiction over child sexual exploitation when this is committed by local residents or when such crimes are committed against victims of Indonesian nationality.

The policy document in Indonesia that touches most directly on OCSEA is the Child Protection Online Road Map. The drafting of this Road Map was initiated by the Ministry of Communication and Information Technology in 2017[48]

A draft of the Road Map was finalised in 2021 but is yet to be formally adopted. There are considerations being made to adopt the Road Map as a presidential decree that will be binding to mandated government agencies for its implementation.

A government representative interviewed for *Disrupting Harm* stated that *"when the Road Map is published it might be easier for us to see which ministry/agency is involved in the initiative."* (RA1-IN-05-A) The Road Map clearly needs to be finalised, formally adopted and actively implemented by engaging all mandated agencies in its implementation.

The National Medium-Term Development Plan (2015–2019) addresses violence against children but does not directly address OCSEA. The National Medium-Term Development Plan 2021–2025, which was under development at the time of the data collection, is now finalised and covers child online protection.[49] Detailed information on how OCSEA is specifically covered was not however available to the research team.

At the regional level, Indonesia adopted the Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN[50] in 2019, as a commitment to improve child protection standards and policies on OCSEA, to enhance the capabilities of professionals, establish a unit specialised in investigating OCSEA-related crimes, strengthen data collection mechanisms, and to raise awareness on the issue and engage with the private sector to combat the crime. In September 2021, Indonesia committed itself to the earlier ASEAN Regional Plan of Action on the Elimination of Violence against Children 2016–2025.

---

43. Government of Indonesia (1999). Penal Code of the Republic of Indonesia. Article 287 and 288.
44. Aljazeera. (2022 April 12). Indonesia passes landmark bill to tackle sexual violence.
45. De Guzman, Chad. (2022, 14 April). After a Teacher Was Convicted of Raping 13 Girls, Indonesia Finally Passed Sexual Violence Reform. Time.
46. See e.g. Qanun Aceh no 6. Year 2014 on Jinayat (Penal Code). "Qanun" are provincial or district regulations/bylaws aimed at implementing Islamic Syariah including in the area of *jinayat* (crime). Law No. 11/2006 gives authority to the province of Aceh as a special autonomous region to implement Islamic Syariah and customary life based on Islam through Qanun. Government of Aceh (2006). Articles 24-33. Law No. 11 of 2006, Article 3.
47. Government of Indonesia (1999). Penal Code of the Republic of Indonesia, Article 5.
48. ASEAN Secretariat. (2019). Ending violence against children in ASEAN Member States: Midterm review of priority areas under the ASEAN Regional Plan of Action on the Elimination of Violence against Children 2016-2025. ASEAN.
49. This information was provided by a representative of the Ministry of National Planning Development during the National Consultation for Indonesia held on 17th March, 2022.
50. ASEAN. (2019). Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN. ASEAN.

1. CHILDREN ONLINE IN INDONESIA

The main focus of the *Disrupting Harm* report series is to present the perspectives of young people, government representatives, service providers and others around the sexual exploitation and abuse of children facilitated or committed through digital technologies. However, it is important to situate these offences within the wider context of children's internet use in Indonesia. This first chapter, therefore, presents a brief overview of children's internet access and the activities enjoyed by the majority of children online before going on to describe the occurrence of riskier online activities and the ways in which these are perceived by internet-using children and their caregivers.

1.1 INTERNET ACCESS AND BARRIERS

Children's access: Sampling data from the *Disrupting Harm* household survey suggest that 92% of 12–17-year-olds in Indonesia are internet users – i.e., they have used the internet within the past three months. Children aged 16–17 were more likely to be internet users (98%) than children aged 12–13 (83%). No differences in internet use were observed by gender or rural/urban location.[51]

Among the internet-using children surveyed, 95% went online at least once a day. As is the pattern in other countries around the world,[52] older children were slightly more likely to report daily internet use than younger children (12–13: 91%; 14–15: 96%; 16–17: 96%) (see Figure 3). Children living in urban areas were somewhat more likely to be frequent users, with 99% of children going online everyday compared to 91% of children in rural areas. No gender differences were observed in frequency of internet use.

Figure 3: Frequency of children's internet use.
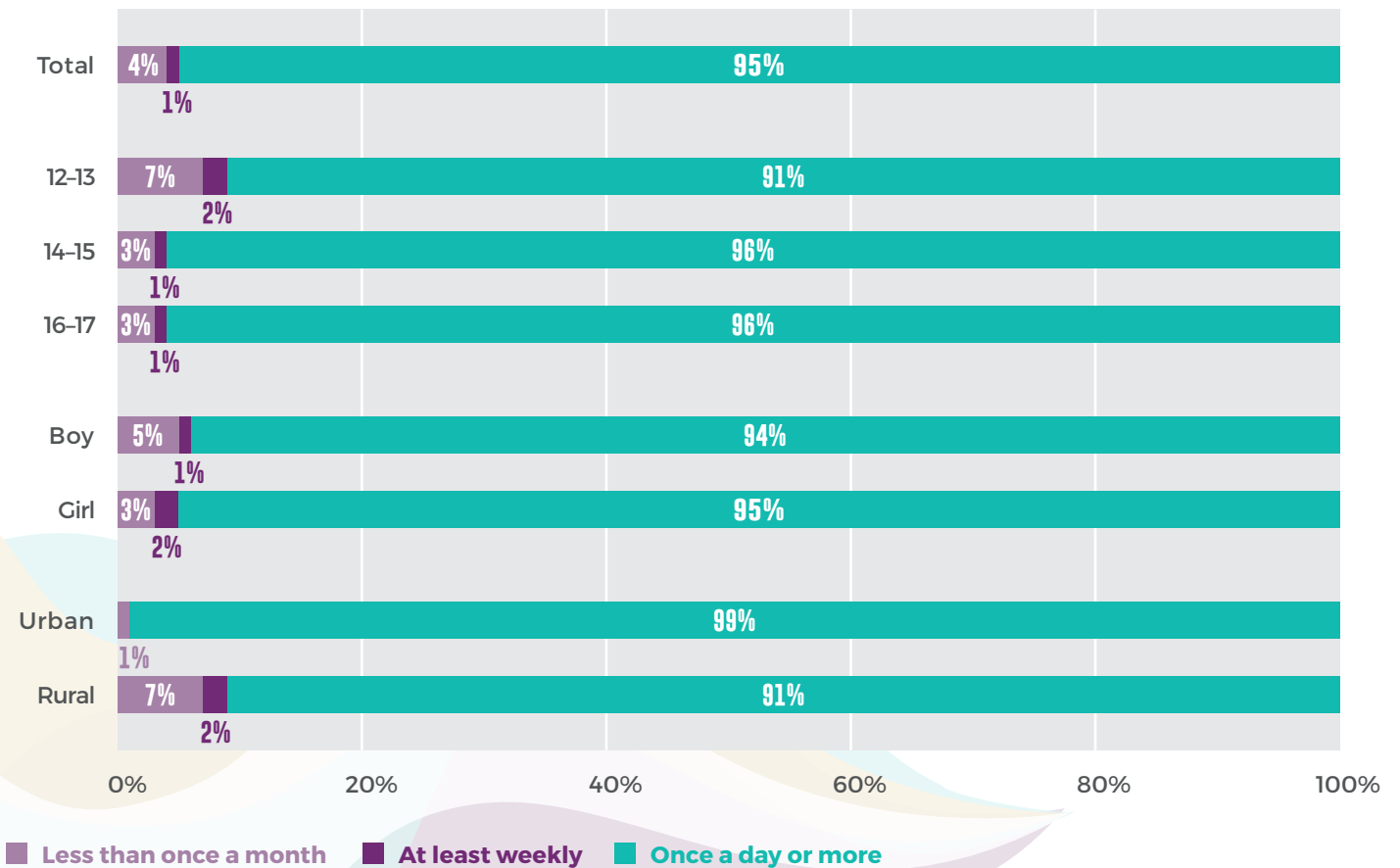
Base: Internet-using children aged 12–17 in Indonesia from the Disrupting Harm study. n = 995.

---

51. While conducting the random walk to identify eligible children to partake in the main survey, we also collected data from every household visited about the number of 12–17-year-old children living there, their gender, age, and whether they had used the internet in the past three months. This allowed us to estimate internet penetration rates for all 12–17-year-old children in Indonesia. n = 995 households.
The question used to determine whether a 12–17-year-old was an internet user: Has [PERSON] used the internet in the last three months? This could include using a mobile phone, tablet or computer to send or receive messages, use apps like Facebook, WhatsApp, Instagram, send emails, browse, chat with friends and family, upload or download files, or anything else that you usually do on the internet.
52. See: Global Kids Online.

Caregivers' access: One caregiver of each child interviewed also took part in the survey.[53] Most of the caregivers were internet users themselves. However, the proportion of internet users was significantly lower among the caregivers than among their children (72% versus 92%). As many as 28% of the caregivers – 64% among those aged 50 and above – had never used the internet. Moreover, among those caregivers who were internet users, only 49% used the internet daily compared to 95% of children. There were no major differences between men and women (see Figure 4).

As many caregivers, particularly older caregivers, have no online experience, or may only have limited experience, it is important to consider the support and knowledge they need, as well as the role that can be played by schools, in guiding their children's use of the internet.

Devices used: As in most other countries, smartphones are by far the most common device used by 12–17-year-old internet users to go online, probably due to their relatively low cost and portability.[54] All of the children surveyed used smartphones, while 6% used computers. Use of computers was higher among older children (12–13: 3%; 14–15: 4%; 16–17: 10%) and children living in urban areas (9%; rural: 3%). There were no notable differences by gender.

This finding is consistent with the widespread use of mobile phones in Indonesia: as of 2019, there were approximately 124 mobile phone subscriptions per 100 inhabitants in Indonesia.[55] By 2025, Indonesia is projected to be the third largest smartphone market globally with an adoption rate of eighty-nine percent.[56]

Figure 4: Frequency of caregivers' internet use.
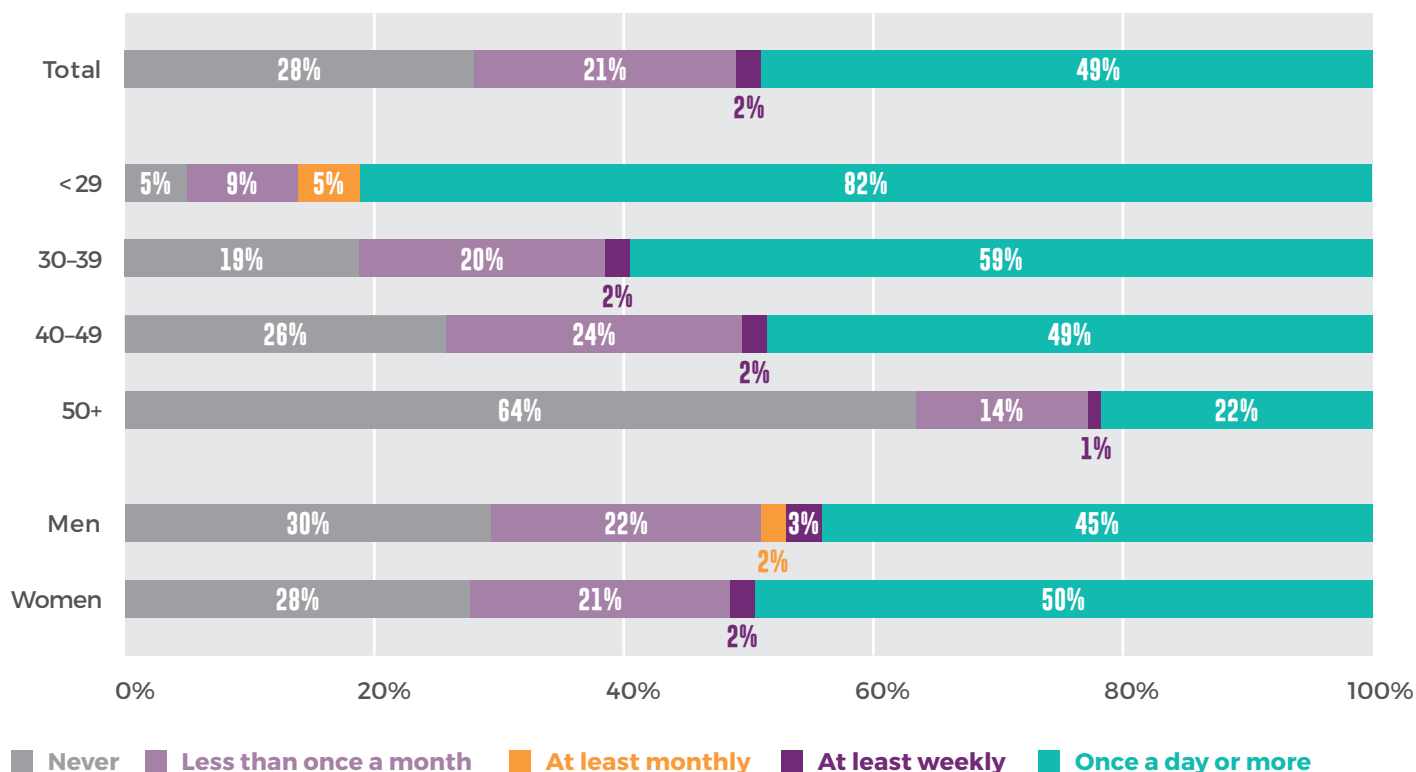
Base: Caregivers of Internet-using children aged 12–17 in Indonesia from the Disrupting Harm study. n = 995.

---

53. The average age of caregivers in the household survey was 42 years old.
54. Kardefelt Winther, D., Livingstone, S., & Saeed, M. (2019). Growing up in a connected world, Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.
55. We are Social, Hootsuite. (2020). Digital 2020: INDONESIA. All the Data, Trends, and Insights you need to Help you understand how people use the Internet, Mobile, Social Media and Ecommerce.
56. GSMA. (2019). The Mobile Economy Asia Pacific 2019. UK: GSMA.

Of the children who used a smartphone, 23% shared it with someone else, a much lower proportion than in many other *Disrupting Harm* countries. The proportion of internet-using children who shared their smartphones with others ranged from 17% among children aged 16–17 to 27% among 12–13-year-olds. In urban areas, 82% of children had their own smartphones compared to 72% in rural areas.

Place of access: All the 12–17-year-old internet users who took part in the household survey (100%) accessed the internet at home, and 62% accessed the internet at school. However, only 13% of children went online at school every day, possibly due to COVID-19-related school closures. More girls (64%) accessed the internet at school than boys (55%). Younger children, aged 12–13, were less likely to access the internet at school than 16–17-year-olds (46% versus 75%). Children in rural areas were slightly more likely to go online at school on a daily basis than children in urban areas (rural: 16%; urban: 10%) and less likely to go online at home on a daily basis (rural: 90%; urban: 98%).

Some of the children surveyed also accessed the internet via public networks at malls (27%) and internet cafés (20%), but for each location only 4% said they did so once a month or more frequently, and only 2% said they did so every day. Seventy-eight percent of children said they go online from some other place not captured in the survey, which might refer to the street, a friend's house or the park, for example.
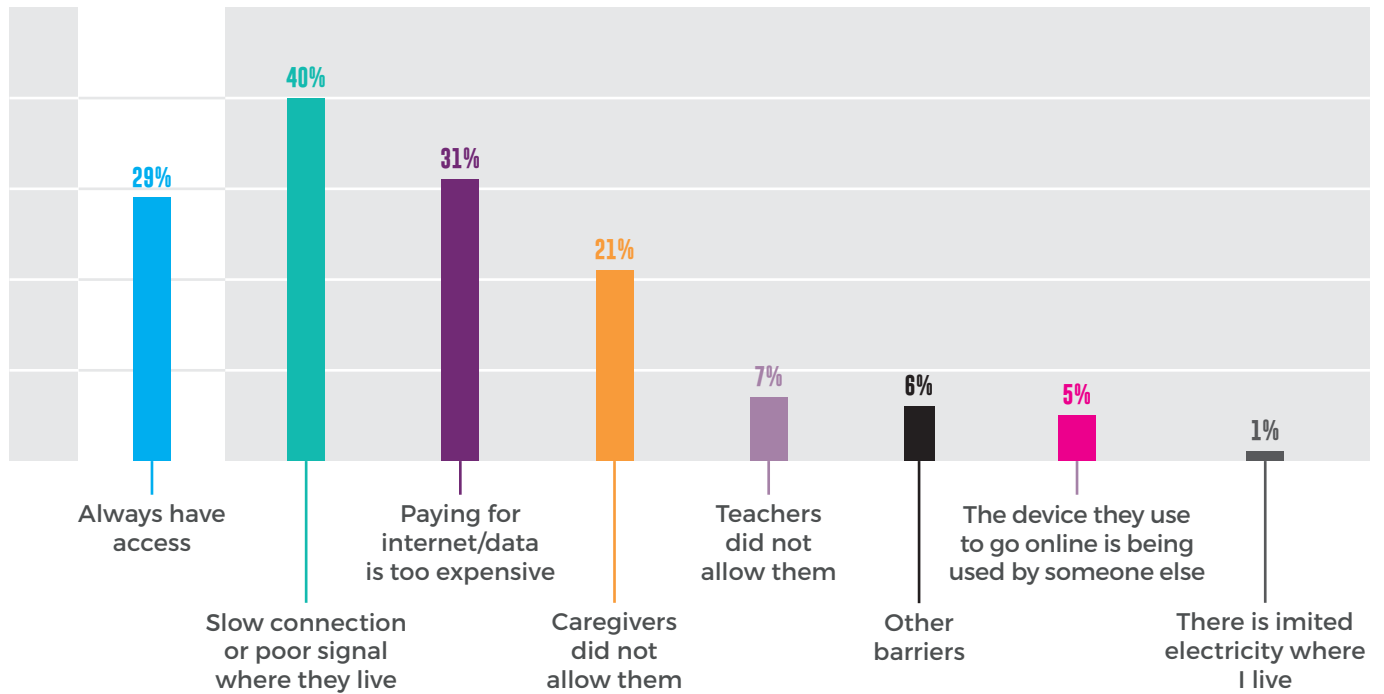
Barriers to access: A majority (70%) of internet-using 12–17-year-olds in Indonesia face barriers in accessing the internet when they want or need it (see Figure 5). A slow connection or poor signal was the most commonly cited reason for limited access, affecting 40% of children. High internet and data costs hindered access for 31% of children, particularly older children (12–13: 27%; 14–15: 32%; 16–17: 33%). This may reflect the fact that older children in the household survey sample use the internet more frequently than younger children and engage in more activities online, therefore requiring more data (see chapter 1.2, below).

> **A majority (70%) of internet-using 12–17-year-olds in Indonesia face barriers in accessing the internet when they want or need it. A slow connection or poor signal was the most commonly cited reason for limited access, affecting 40% of children.**

Children also reported restrictions to internet access imposed by their caregivers and, to a lesser extent, teachers. Younger children were somewhat more likely to cite parental restrictions as a barrier to access (12–13: 26%; 14–15: 21%; 16–17: 15%), as were children in rural areas (23%; urban: 18%). Parental restrictions may be more prevalent in rural areas due to demands on the children's time, or be related to other barriers such as costs, or the need for others to use the device.

While a restrictive approach might reduce children's exposure to online risks in the short term, it also reduces their familiarity with the online environment in the long term. Such a response might further be viewed as a form of punishment by children and may deter them from voicing their concerns about unwanted experiences online. Some level of parental restrictions may be protective if part of broader strategies whereby caregivers' engagement with children centres on guidance and support in case they encounter harm online. (see page 34 for more on parental support).

Figure 5: Barriers to access for internet-using children.

Always have access: 29%
Slow connection or poor signal where they live: 40%
Paying for internet/data is too expensive: 31%
Caregivers did not allow them: 21%
Teachers did not allow them: 7%
Other barriers: 6%
The device they use to go online is being used by someone else: 5%
There is imited electricity where I live: 1%

Base: Internet-using children aged 12–17 in Indonesia. n = 995.

1.2 CHILDREN'S ACTIVITIES ONLINE

Almost all the children surveyed reported that they used the internet for schoolwork, which likely reflects increased reliance on the internet during school closures and national lockdowns due to COVID-19 (see Figure 6). A vast majority of children also used instant messaging (86%) and social media (71%). Other popular activities included talking to family or friends who live further away (62%), watching videos (61%), watching a livestream (49%) and playing video games (43%).

Older children and girls engaged in all these activities in somewhat higher proportions than younger children and boys, with the exception of online gaming. Forty-six percent of children aged 12–13 reported playing online games as compared to 38% of children aged 16–17. Online gaming was much more common among boys (70%) than girls (20%), a trend observed in other *Disrupting Harm* countries.

The survey data also indicate that, in comparison to children in urban areas, smaller proportions of children in rural areas engaged in all activities on a weekly basis. For instance, 63% of children in rural areas used social media on a weekly basis as compared to 79% of children in urban areas.

Of note, in the context of COVID-19, social media platforms such as Facebook, WhatsApp and LINE have become popular platforms for digital learning.

They are used for educational purposes by serving as mediums for communication and the sharing of educational materials like assignments and notes, and are increasingly preferred over EdTech platforms that curate specific courses and material but also require greater bandwidth and incur higher data costs.[57] In an INOVASI study conducted in April 2020 involving 221 participants mostly from *Sekolah Dasar* (elementary schools), it was found that, of the 24% that studied online, 98% did so through instant messaging (WhatsApp, LINE, or Facebook), and very few did so through public online learning platforms like Rumah Belajar, or private ones such as Ruangguru and Zenius.[58]

Figure 6 provides a greater understanding of how 12–17-year-olds in Indonesia use the internet and the activities they enjoy online. It is worth considering that these categories are not intended to be mutually exclusive – for example, a child could go online to watch a video as part of their schoolwork.

57. UNICEF Indonesia. (2021). Situational analysis on digital learning landscape in Indonesia.
58. INOVASI (2020). Teacher Survey. Indonesia.

Figure 6: Activities children engage in online at least once a week.

Children's online activities	Total	12–13	14–15	16–17	Boy	Girl	Urban	Rural
School work	91%	89%	91%	93%	88%	94%	94%	89%
Used instant messaging	86%	79%	86%	92%	85%	87%	91%	82%
Used social media	71%	63%	70%	78%	68%	73%	79%	63%
Talked to family and friends who live further away	62%	55%	61%	68%	57%	66%	67%	57%
Watched videos	61%	54%	62%	66%	59%	63%	69%	53%
Watched a livestream	49%	41%	51%	53%	45%	52%	54%	44%
Played online games	43%	46%	45%	38%	70%	20%	52%	35%
Searched for new information	41%	35%	39%	48%	36%	45%	48%	34%
Looked for news	30%	17%	27%	42%	27%	32%	37%	23%
Looked for information about work or study opportunities	23%	16%	21%	32%	23%	24%	29%	18%
Participated in a site where people share their interests	21%	15%	21%	26%	24%	19%	27%	15%
Looked for information or events in the local neighbourhood	20%	12%	22%	26%	16%	24%	23%	18%
Looked for health information	19%	14%	21%	23%	15%	23%	23%	16%
Followed celebrities and public figures on social media	18%	14%	17%	23%	13%	22%	25%	12%
Created their own video or music	14%	11%	15%	16%	11%	17%	16%	13%
Sought emotional support	12%	8%	13%	15%	11%	13%	14%	10%
Discussed political or social problems	9%	6%	10%	11%	8%	10%	12%	7%
Created a blog or website	6%	6%	8%	6%	6%	7%	8%	5%

Base: Internet-using children aged 12–17 in Indonesia. n = 995.

" The survey data also indicate that, in comparison to children in urban areas, smaller proportions of children in rural areas engaged in all activities on a weekly basis. For instance, 63% of children in rural areas used social media on a weekly basis as compared to 79% of children in urban areas. "

1.3 PERCEPTIONS AND EXPERIENCES OF RISKY ONLINE ACTIVITIES

Discussion of online risks often hinges upon adult-centric perceptions. To help us understand children's perceptions, they and their caregivers were asked about their engagement in, and perceptions of, various risky online activities.

1.3.1 Contact with strangers online and in person
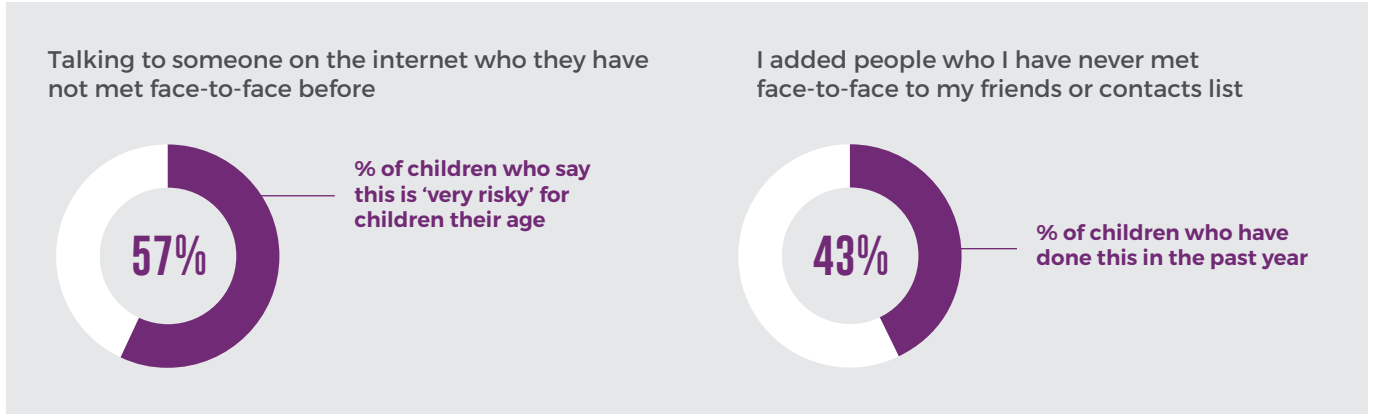
Communicating with strangers online

A common concern around children's online use is their exposure to 'stranger danger'. In the household survey, 79% of the caregivers rated "talking to someone on the internet whom they have not met face-to-face before" as 'very risky' for children. Yet only 57% of the children rated this activity as 'very risky' for children of their age. Children aged 12–15, particularly girls, were most likely to describe talking online with a person they did not know as 'very risky'.

Similarly, 69% of the children surveyed, and again girls in particular, thought it 'very risky' for children to send their personal information to someone they had never met face-to-face, compared to 84% of the caregivers. Older caregivers were more concerned about all the risks that were asked about.

While most of the internet-using children recognised that interacting with strangers carries *some* level of risk, 12% felt that there was no risk at all, suggesting a lack of awareness by some children about how speaking to strangers online might lead to harmful outcomes.

Figure 7: Level of risk attributed by children to speaking to someone unknown to the child online, by age.

Speaking with online strangers – children's risk perceptions and behaviour.

Talking to someone on the internet who they have not met face-to-face before

57%

% of children who say this is 'very risky' for children their age

I added people who I have never met face-to-face to my friends or contacts list

43%

% of children who have done this in the past year

Base: Internet-using children aged 12–17 in Indonesia. n = 995.

Sharing personal information with online strangers – children's risk perceptions and behaviour.

Sending personal information (e.g., their full name, address or phone number) to someone they have never met face-to-face

69%

% of children who say this is 'very risky' for children their age

I sent my personal information (e.g., my full name, address or phone number) to someone I have never met face-to-face

29%

% of children who have done this in the past year

Base: Internet-using children aged 12–17 in Indonesia. n = 995.

Disrupting Harm in Indonesia – Evidence on online child sexual exploitation and abuse

Disrupting Harm evidence shows that children do engage with new people online and that some children go on to meet these people in person. For example, 43% of children said they had added people they had never met face-to-face to their contact lists in the past year. This figure ranged from 31% for 12–13-year-olds to 51% for 16–17-year-olds. There was no notable difference by gender. Twenty-nine percent of the children had shared their personal information with someone they had never met face-to-face.

Meeting online acquaintances in person

In the household survey, 60% of the children and 80% of their caregivers rated "going to meet someone face-to-face that they first got to know online" as 'very risky' for children. Girls were slightly more likely than boys to regard this as high-risk behaviour (64% versus 56%). Among caregivers, the older ones were more likely to consider such behaviour 'very risky' (aged 29 or under: 67%; aged over 50: 85%). However, close to one in ten children viewed this behaviour as 'not risky at all'.

There are clearly incongruences between children's and caregivers' perceptions. Meeting someone you do not know face-to-face for the first time can be very risky. But there are different types of such encounters, such as in connecting with new children in the community first online and then in person, or going to group events with caregivers.

In actual fact, 11% of the children surveyed had met someone in person whom they had first met online in the past year. According to children, many of these encounters did not result in immediate harm and most respondents described being pleased about the outcome (see Figure 8). Research done across more than 30 countries around the world has produced similar findings.[59,60]

Although these encounters tended to be positive for children in our survey, this remains a risky activity, with potentially harmful outcomes.

Figure 8: How children felt the last time they met someone face-to-face who they had first got to know online.
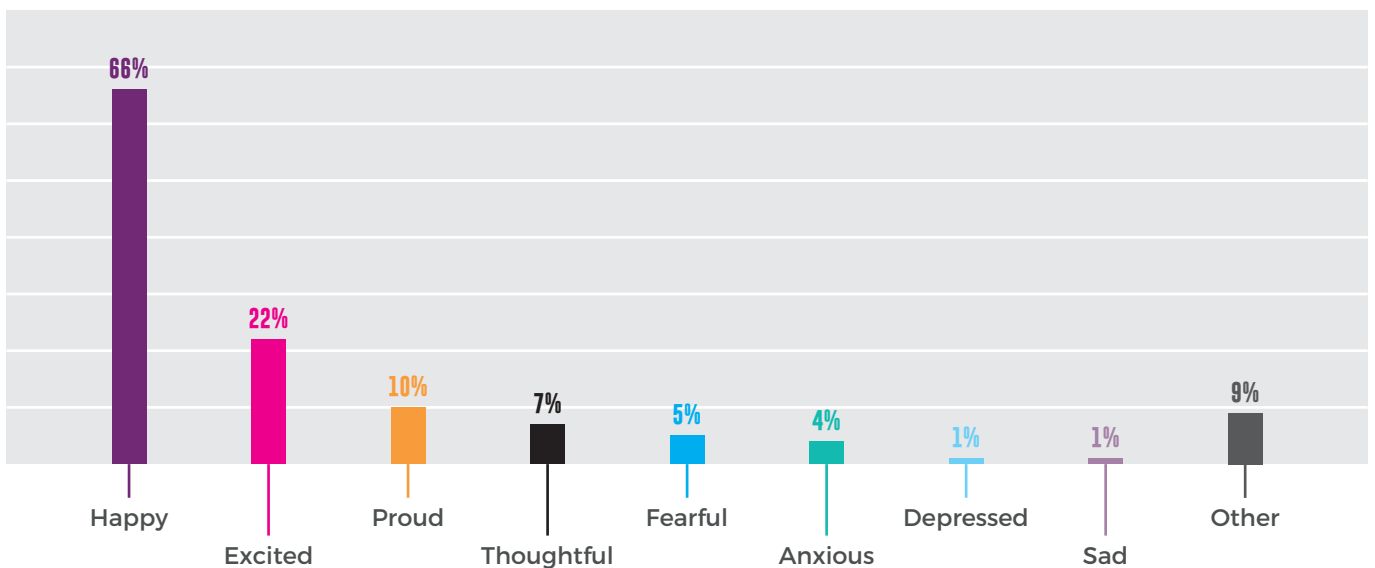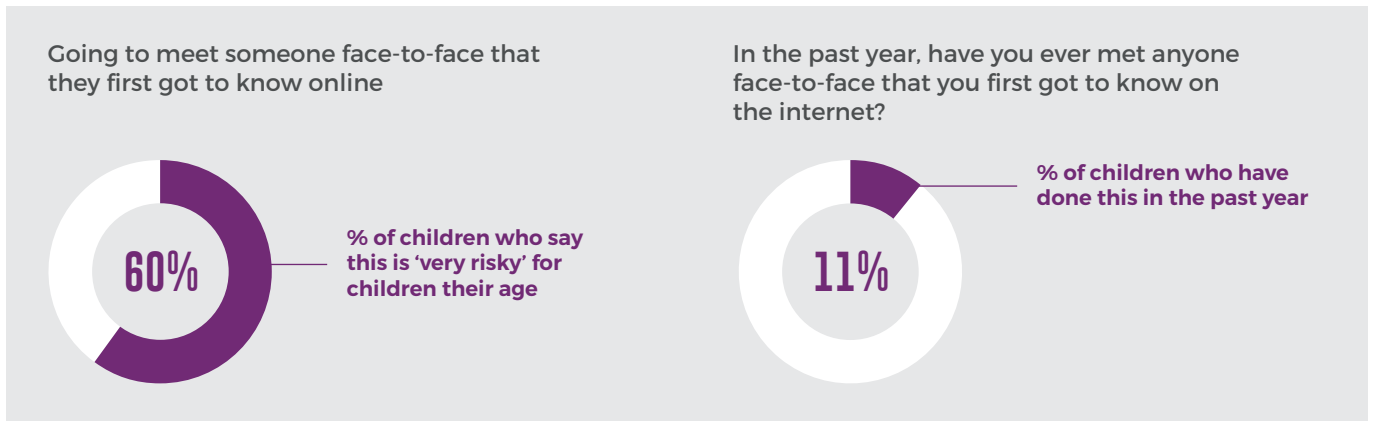

Base: Children who, within the past year, have met someone face-to-face whom they first got to know on the internet. n = 105

59. Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). Global Kids Online Comparative Report, *Innocenti Research Report.* Florence: UNICEF Office of Research - Innocenti.
60. Smahel, D., Machackova, H., et al. (2020). EU Kids Online 2020: Survey results from 19 countries. Florence: UNICEF Office of Research – Innocenti.

Figure 9: Meeting online strangers in person – children's risk perceptions and behaviour.

Going to meet someone face-to-face that they first got to know online

60%

% of children who say this is 'very risky' for children their age

In the past year, have you ever met anyone face-to-face that you first got to know on the internet?

11%

% of children who have done this in the past year

Base: Internet-using children aged 12–17 in Indonesia. n = 995

Empowering Caregivers to Guide their Children's Internet Use

Caregivers can be a first line of defence in protecting children from online harm – but only if they have a grasp of basic digital skills, are aware of online risks, avoid being overly restrictive and focus on equipping their children to stay safe online.

With respect to internet use and digital skills, older caregivers in Indonesia seem to be at a disadvantage. Sixty-four percent of the caregivers aged 50 or above included in the household survey had never used the internet, and only 22% used it on a daily basis. These caregivers also had the weakest digital skills. For example, only 20% said they knew how to report harmful content on social media, compared to 57% of caregivers aged 29 or younger.

When faced with constant messaging that greater access to technology and the internet increases children's vulnerability to OCSEA – a view shared by 48 out of the 50 frontline service providers surveyed for *Disrupting Harm* – caregivers might instinctively react by restricting their children's internet use in a bid to protect them. In the household survey, 55% of the caregivers said they would restrict their child's internet access if their child was bothered by something online.

Interestingly, it was the youngest caregivers, aged 29 or younger, who were most likely to give this response (64%, compared to 52% of caregivers older than 50).

While a restrictive approach might reduce children's exposure to online risks in the short term, it also reduces their digital skills and familiarity with the online environment in the long term. Furthermore, such a response might be viewed as a form of punishment. This could make them less likely to voice concerns about harm or other unwanted experiences they encounter online.

On the other hand, *supportive engagement* by adults has been associated with positive skills development for children in other countries.[61] Supportive engagement could include engaging in activities together, talking to children about their internet use, and educating them about the risks that exist online and how best to avoid them. Engaging with children in this way allows them to reap the benefits of the many useful activities and skills that the internet has to offer while providing parental guidance and support in case they encounter any kind of harm online.

61. Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). Global Kids Online Comparative Report, *Innocenti Research Report.* Florence: UNICEF Office of Research - Innocenti.

It is therefore encouraging that a majority of children in Indonesia say that their caregivers support their internet use. For example, 82% of the children surveyed said their caregivers suggest ways for them to stay safe online and 71% said their caregivers help them if they are bothered by something on the internet.

According to *Disrupting Harm* data, on average only 32% of caregivers in Indonesia said they knew more about the internet than their child, with stark differences between age groups (Figure 10). Ten percent of caregivers aged 50 and above further indicated that they would not be able to help 'at all' should their child be bothered online.

Figure 10: Caregivers who say they know more about the internet than their child, by age.

29 or younger
57%

30–39
40%

40–49
29%

50+
4%
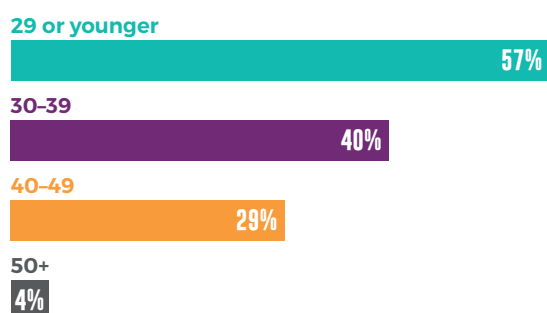
Base: Internet-using caregivers in Indonesia. n = 719.

Caregivers who are not internet users or who go online less frequently than their children might worry that they do not have enough knowledge to guide them. However, they can still talk to their children about what they do online and provide an open and supportive home environment where children feel comfortable disclosing negative experiences. Among the caregivers surveyed, 52% said they would talk to their child if something bothered them online. It is important to provide these caregivers in particular with the knowledge and support they need to do this. Schools and parental education programmes can play an important role in this area.

Asked about the channels through which they received guidance on how to support their children's internet use and keep them safe, 65% of the caregivers in the household survey mentioned family or friends. Others cited their children's school (39%) or television (32%) as sources of information. These were also the channels through which the caregivers said they would *prefer* to receive guidance. These channels could therefore be leveraged to disseminate awareness messages or educational programmes about how caregivers can empower children to use the internet safely and effectively.

"
Among the caregivers surveyed, 52% said they would talk to their child if something bothered them online. It is important to provide these caregivers in particular with the knowledge and support they need to do this.
"

1.3.2 Seeing sexual images online

Seeing sexual content was the top *internet-related* concern that caregivers had regarding their children.

Ninety percent of the caregivers, as well as 78% of the children surveyed, considered seeing sexual images or videos online 'very risky' for children – higher percentages than for those who considered it 'very risky' to meet an online acquaintance face-to-face.

This concern around children seeing sexual images or videos may reflect the prevalence of discomfort around openly discussing sex and sexuality in general in Indonesia (see chapter 2.4). Such concerns may also stem from social norms which discourage such activities and from existing legislation whereby viewing pornography is illegal.[62]

All but one of the 50 frontline workers surveyed regarded 'access and exposure to pornography' as a factor increasing children's vulnerability to OCSEA, ahead of issues like migration, experiences of family and community violence, or living on the street (see figure 22 in 2.4.1).

The different ways children access sexual content online can have different consequences and may require diverse interventions for prevention and response. For instance, accidental or intentional glimpses of sexual content cannot be equated with children's exposure to sexual images as part of a grooming process with intent to harm (see chapter 2.2). While viewing violent or degrading sexual content can serve to normalise harmful gender norms and sexual behaviour, seeing pornography online appears to be an increasingly present experience for young people.[63] Addressing both phenomena is needed.[64]

Figure 11: Caregivers' top concerns regarding their children.
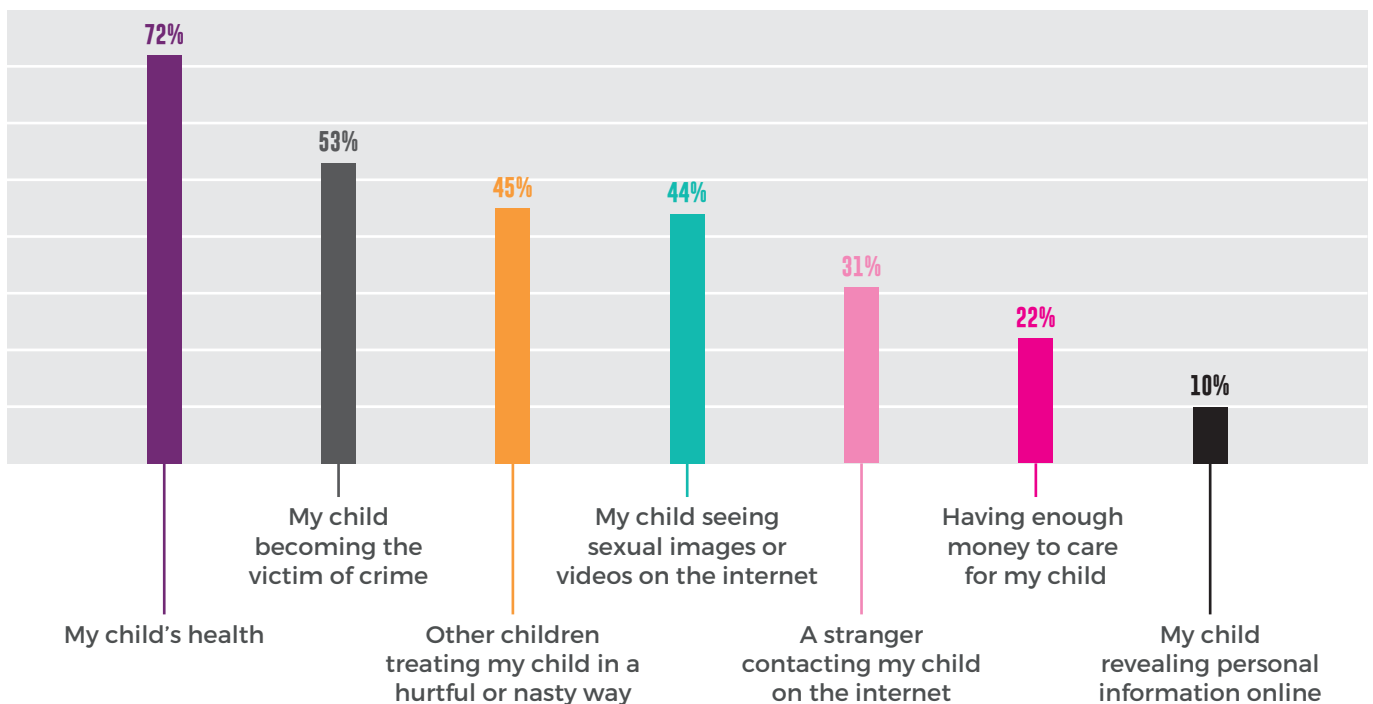
Base: Caregivers of internet-using children aged 12–17 in Indonesia. n = 995.

---

62. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Section 6.
63. See for example: Crabbe, M. & Flood, M. (2021). School based Education to Address Pornography's Influence in Young People: A Proposed practice framework. American Journal of Sexuality Education, 16(1), 1-37.
64. Bell, C. (2017). An Overview of Research on the Impact that Viewing Pornography has on Children, Pre-Teens and Teenagers. Bravehearts.

Children's experiences: According to past research, Indonesia is a country where children are particularly likely to encounter sexual content online.[65,66] However, the household survey did not confirm this. Nevertheless, 24% of internet-using children reported they had seen sexual images or videos online at least once in the past year. Nine percent reported actively looking for such material online and 22% had been exposed to sexual images or videos when they did not expect it. These numbers are lower than in other *Disrupting Harm* countries and may indicate a level of under-reporting, possibly because of discomfort discussing this sensitive topic or because viewing pornography is criminalised in Indonesia.

Older children and boys were somewhat more likely to be exposed to sexual content online, both intentionally and accidentally. For example, 24% of boys said they had come across sexual content online by accident, 69% said they hadn't, and 6% said they didn't know or preferred not to answer the question. Among girls, these percentages were 19%, 78% and 3% respectively.

Fifty-three percent of the children who had seen sexual images or videos online involuntarily said they had seen them in advertisements (e.g. pop-ups). Thirty-eight percent had come across sexual content via social media feeds and 20% while using search engines, whereas 12% received the content via direct messaging apps. Girls (60%) were more likely to have seen sexual content through advertisements than boys (60% versus 47%), and boys were more likely than girls to have been sent the images via direct messaging apps (14% versus 9%). Younger children exposed to such images or videos were more likely than older children to have seen them on social media (12–13: 44%; 16–17: 37%) or received them in direct messages (12–13: 17%; 16–17: 12%).

1.3.3 Making and sharing self-generated sexual content

Seventy percent of the children and 79% of the caregivers surveyed agreed with the statement "It is wrong for a person to take naked images or videos of themselves".

Seeing or sharing sexual images or videos were the online activities that were most often perceived as 'very risky' by both the children and the caregivers surveyed. Sending a sexual image or video to someone online was considered 'very risky' by as many as 80% of children and 90% of caregivers. As with other online activities, younger children aged 12–13 were the least likely to assess this activity as very risky (73% versus 85% among children aged 16–17). In practice, only 1% of the children in the household survey (11 children) said they had shared naked pictures or videos of themselves online in the past year. Older children aged 16–17 were somewhat more likely to report this. These figures are lower than in most other *Disrupting Harm* countries but could be under-reported due to common discomfort around openly discussing sex or potential criminal liability.

When asked why they had shared naked images or videos of themselves, five of the eleven children gave "flirting or having fun" as their explanation (or one of their explanations). Two children preferred not to say why they had shared such content, and another two said they did not know why they had done it.
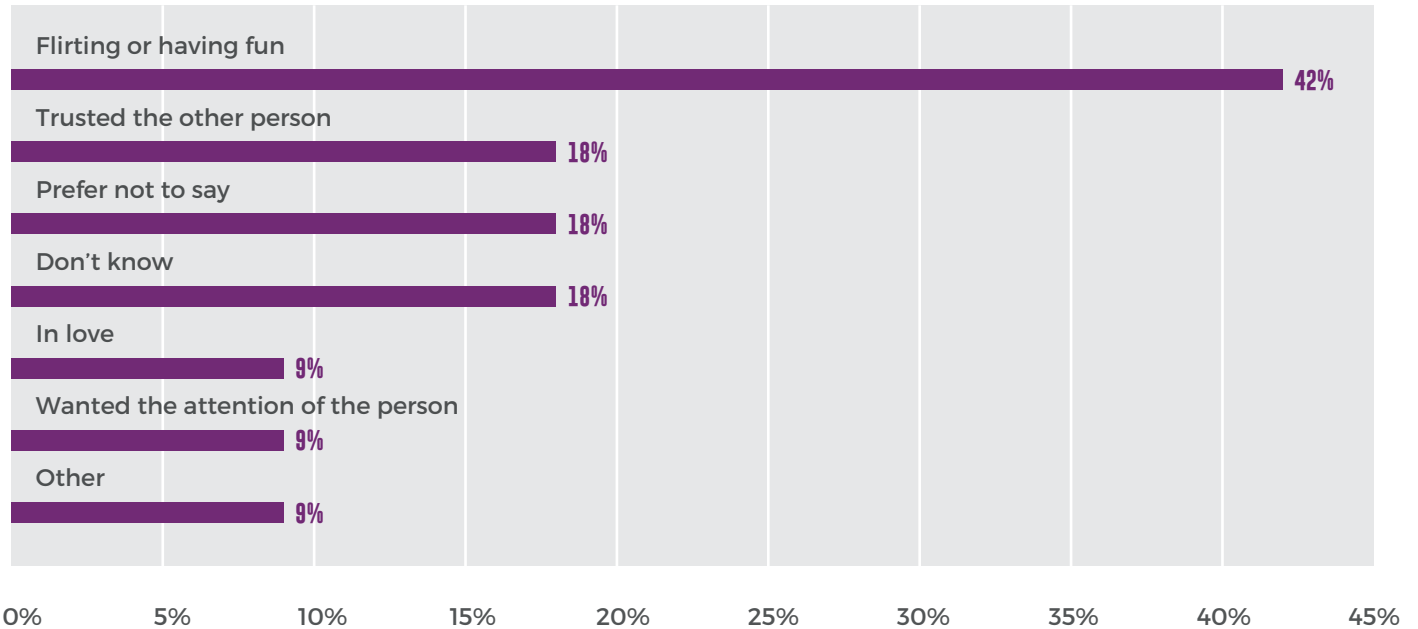
Consistent with the reasons which they gave for sharing the images, the 11 children had mostly shared the images or videos with a romantic partner or someone else they knew in person. Some children said that they did not know whom they had shared the content with or preferred not to say – perhaps because they felt uncomfortable discussing the topic. One child shared the images with someone they had met online who had no prior connection in their life.

65. ECPAT Indonesia. (2014). The Scope and Magnitude of Online Sexual Abuse of Children in Indonesia.
66. Pratama, B., Sofian, A., & Talerico, C. (2018). Weighting Approaches on Online Sexual Abuse of Children: Cultural Prevention or Crime-Based Enforcement? Udayana Journal of Law and Culture, 2(2), 191-219.

Figure 12: Reasons given by children for sharing naked images or videos of themselves.

Reason	Percentage
Flirting or having fun	42%
Trusted the other person	18%
Prefer not to say	18%
Don't know	18%
In love	9%
Wanted the attention of the person	9%
Other	9%

Base: Children who have shared naked images or videos of themselves in the past year. n = 11.

The Rise in Self-Generated Sexual Content Involving Young People

The increasing use of technology is leading to shifts in notions of privacy and sexuality among children in some parts of the world, particularly adolescents.[67] Forms of behaviour that are increasingly normal to young people can be bewildering for adults who grew up in a different time. For instance, video live-streaming is common, whether among small private groups of friends or anonymous public audiences. While much of the live-streaming is harmless, there is an increase in producing and sharing of self-generated sexual content, which can bring significant risks.[68]

The sharing of self-generated sexual content by children is complex and includes a range of different experiences, risks, and harms. As the *Disrupting Harm* data show, some self-generated content is shared with others because children are in love or having fun; globally, such exchanges are increasingly becoming part of young people's sexual experiences. However, as the Indonesia data for *Disrupting Harm* illustrates, the creation and sharing of self-generated sexual content can be coerced through threats or by peer pressure. (see chapter 2.2)

---

67. Livingstone, S. & Mason, J. (2015). Sexual Rights and Sexual Risks among Youth Online: A review of existing knowledge regarding children and young people's developing sexuality in relation to new media environments. London: European NGO Alliance for Child Safety Online.
68. Thorn & Benson Strategy Group. (2020). Self-Generated Child Sexual Abuse Material: Attitudes and experiences.

There can be negative consequences for children sharing *any* sexual content including in cases where sharing is not coerced. Material shared willingly may not cause harm at first, but there remains a risk if it is later shared beyond the control of the person who created it. Once it exists, such content can also be obtained deceptively or using coercion and be circulated by offenders perpetually.[69,70]

In Indonesia, a substantial proportion of 12–17-year-olds seem to be aware that producing and sharing sexual content can carry risks for children. In addition, relatively few children appear to engage in this kind of behaviour. Nevertheless, the numbers of children sharing sexual images, for whatever reason, could be substantial if scaled-up to the total population of internet-using children in the country. The possible risks that sharing sexual content online entails should be central to all discussions with children about their internet use – at home, at school, and in the community.

It can be difficult for children to seek help if sexual content involving them is shared with others without permission, partly owing to the fear of victim blaming. In Indonesia, the household survey showed that a large majority of children (76%) and caregivers (85%) believe that, should a self-generated image or video be shared further, it is the victim's fault. When self-generated content is shared without permission, reluctance or inability to seek help may lead to further harm for children.

Finally, victims who are coerced or manipulated into sharing sexual content may be reluctant to report because they could expose themselves to criminalisation under the generalised ban on pornography.[71] This adds an extra layer of complexity to the issue of self-generated sexual content by young people in Indonesia.

Figure 13: Mapping the consequences of sharing self-generated sexual content involving children.
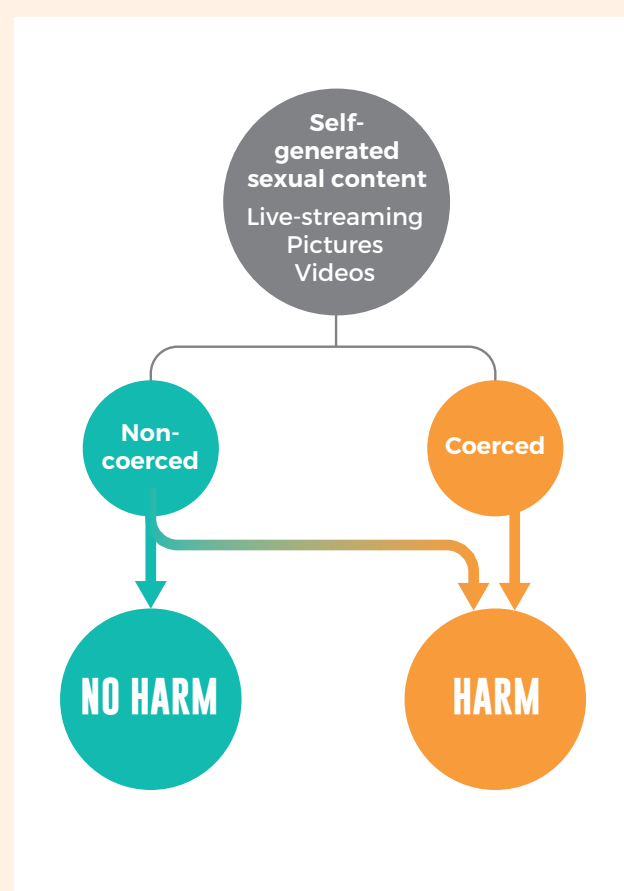
69. Bracket Foundation. (2019). Artificial Intelligence: Combating Online Sexual Abuse of Children. US: Bracket Foundation. 10.
70. EUROPOL. (2019). Internet Organised Crime Threat Assessment 2019. Netherlands: EUROPOL.
71. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Sections 5, 6 and 29.

1.3.4 Knowledge and skills for online safety

A 2016 survey conducted in selected Asia-Pacific countries indicated that children in Indonesia rank highest in preventative strategies online (e.g., modifying privacy settings and communicating problematic interactions to a parent, sibling or peer) but lowest in disengaging from upsetting situations.[72]

Forty-three percent of the internet-using children who took part in the household survey in Indonesia (46% of girls and 39% of boys) said they had received information about how to stay safe online. However, 41% said that they had never received such information. The remainder said they did not know or did not answer the question – perhaps suggesting that they had no idea what such information might look like. Only 37% of children aged 12–13 had received online safety information compared to 51% of 16–17-year-olds.

Questioned about their skills for staying safe online, the children surveyed seemed to be more confident in their ability to judge situations than in their technical skills. A majority expressed confidence in their ability to judge which images of themselves or their friends to share online (75%) and when to remove people from their contact lists (74%). However, the proportions of children who said they knew how to change privacy settings, report harmful content on social media and check whether a website can be trusted were distinctly lower, at 58%, 49% and 36% respectively.

> **Forty-three percent of the internet-using children who took part in the household survey in Indonesia (46% of girls and 39% of boys) said they had received information about how to stay safe online. However, 41% said that they had never received such information.**

Without such practical digital skills, children are not as well equipped as they could be to stay safe online. As an important stakeholder, industry – including global platforms and internet service providers – could take a stronger role in promoting digital skills development and improving online safety for children.

Younger children were less likely to know how to operate such security features than older children, and children in rural areas appeared to be somewhat less digitally skilled than those living in urban areas. For example, only 49% of children in rural areas knew how to change their privacy settings compared to 68% of children in urban areas. Similarly, fewer children in rural areas would know how to report harmful content on social media (44%; urban: 54%). No significant gender differences were observed in the data.

While it is encouraging to note that many children know how to operate online safety features, existing research indicates that young people may voluntarily compromise their own safety online, including by sharing passwords with friends or romantic partners, as a sign of trust or intimacy. This phenomenon was also observed by UNICEF in Indonesia, where a number of girls spoke about how they used privacy settings to demonstrate trust in their boyfriends.[73]

72. Rimini, M., Howard, C., & Ghersengorin, A. (2016). Digital Resilience: Empowering Youth Online. Brussels: Think Young.
73. UNICEF East Asia and the Pacific Regional Office and Centre for Justice and Crime Prevention. (2020). Our Lives Online: Use of social media by children and adolescents in East Asia - opportunities, risks and harms. Thailand: UNICEF East Asia and the Pacific Regional Office.

2. ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN INDONESIA

Following on from children's perceptions of, and participation in, various risky online practices, this chapter will turn to the threat of online child sexual exploitation and abuse (OCSEA) in Indonesia. National crime data was not available from national law enforcement authorities, but this chapter draws on a variety of sources – including foreign law enforcement data, mandated reports from U.S.-based technology companies to NCMEC related to Indonesia, surveys with frontline workers and surveys, interviews and conversations with children themselves – in order to create a well-rounded presentation of the nature of these crimes against children.

While foreign law enforcement data and mandated reports from U.S.-based technology companies to NCMEC cannot be validated by Indonesian law enforcement in the same way as internally approved statistics are, the information contained in them might be helpful in interpreting the data found by the _Disrupting Harm_ project. This chapter therefore estimates the occurrence of certain instances of OCSEA based on data from NCMEC CyberTipline and foreign law enforcement agencies (chapter 2.1) and children's self-reported experiences (chapter 2.2 and 2.3) and ends with insights concerning victim and offender profiles (chapter 2.4) and reasons for non-disclosure (chapter 2.5).

For several reasons, estimates are not intended to provide a conclusive picture of the prevalence of OCSEA. Firstly, there is the absence of national crime statistics and case studies from the law enforcement authorities. Secondly, with respect to the household survey, a degree of under-reporting could be expected due to privacy concerns, discomfort when talking about sex, and stigma around sexual exploitation and abuse. Some children may also fear legal self-incrimination since practices such as the production, possession and viewing of pornography are criminalised.[74] Furthermore, in households where sexual abuse occurs, researchers would be less likely to be given permission to talk to the children for such a survey.

The survey only included internet users and children who live at home and, therefore, it may not represent vulnerable populations such as children engaged in migration, children deprived of liberty, children in institutions or street-connected children. Finally, many estimates are based on the analysis of sub-samples of the survey data which are small as OCSEA is still a rarely reported phenomenon, resulting in a larger margin of error.

While _Disrupting Harm_ has full confidence in the data and the quality of the sample obtained, the challenges of researching specific and sensitive phenomena mean the loss of some precision in the final estimate. For these reasons, it is suggested that the reader interprets the findings in this chapter as _a good approximation_ of the occurrence of certain crimes against children related to OCSEA in Indonesia and the extent to which internet-using children in Indonesia are subjected to OCSEA.

---

74. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Sections 5, 6 and 29.

2.1 LAW ENFORCEMENT DATA

2.1.1 Recorded OCSEA offences

Data on recorded national crimes statistics on OCSEA was requested directly from the Indonesian law enforcement authorities via the INTERPOL National Central Bureau Jakarta. However, no data were provided during the research timeline.[75]

Other related data sources (data from NCMEC CyberTipline and foreign law enforcement agencies) which are beyond the specific prescribed methodological scope of the *Disrupting Harm* research activities may be contextually helpful in establishing data on OCSEA prevalence and law enforcement activity in Indonesia. While these external studies cannot be validated by Indonesian law enforcement in the same way as internally approved statistics are, the information contained in them might be helpful in interpreting the data found by the *Disrupting Harm* project; likewise, any discrepancies identified between *Disrupting Harm* and external studies might illustrate the challenges faced by law enforcement in identifying and addressing OCSEA, and serve as motivation for further capacity building and operational support.

The data from NCMEC CyberTipline and foreign law enforcement agencies presented in this chapter was obtained as a result of requests made to these institutions by INTERPOL on behalf of the Indonesian law enforcement authorities.

2.1.2 International OCSEA detections and referrals

Reports to the U.S.-based National Center for Missing and Exploited Children (NCMEC)

NCMEC provided data about CyberTips concerning suspected child sexual exploitation in Indonesia for the years 2017 to 2019. U.S. federal law requires that U.S.-based electronic service providers (i.e., technology companies) report instances of suspected child exploitation to NCMEC's CyberTipline. For providers not based in the U.S., this reporting is voluntary. Not all platforms report suspected child exploitation to NCMEC. There is therefore an information gap concerning the prevalence of OCSEA on a number of platforms popular in *Disrupting Harm* focus countries.[76]

Both the number of reports and the percentage of global reports that relate to Indonesia are noticeably higher than that for other *Disrupting Harm* focus countries. As a point of comparison, the number of reports pertaining to Indonesia in 2019 was slightly higher than for the Philippines, and nine times higher than for Cambodia for the same reporting year. At the same time, the number of reports for Indonesia does not appear to have increased as sharply over the reporting period as the global total and was subject to a more marked reduction in 2019. This trend does not necessarily indicate low growth rate in offending; it may well indicate a move in Indonesia away from the misuse of those platforms that report suspected child exploitation to NCMEC, thereby raising the question of what platforms or channels OCSEA offenders might be shifting to.

Figure 14: CyberTips concerning suspected child sexual exploitation in Indonesia.

	2017	2018	2019	% Change 2017 to 2019	% Change 2018 to 2019
Indonesia	727,494	1,223,972	840,221	15%	-31%
Global Total	10,214,753	18,462,424	16,987,361	66%	-8%
Indonesia % of Global Total	7.12%	6.63%	4.95%		

Base: CyberTip data provided by NCMEC.

---

75. While COVID-19 affected the data collection for all *Disrupting Harm* countries, the effect was felt particularly hard in Indonesia, where levels of various types of OCSEA are anecdotally known to be quite significant. As mentioned above, Indonesian law enforcement was asked to identify and contribute data, and all following conversations and discussions involving the data were carried out remotely. Unfortunately, the global health concerns at the time did not allow for on-site queries for further clarification or supplemental categorisation.
76. It is important to note that country-specific numbers may be impacted by the use of proxies and anonymisers. In addition, due to variance of law, each country must apply its own national laws when assessing the illegality of the reported content.

2.1 LAW ENFORCEMENT DATA

Analysis of the types of incidents reported to NCMEC reveals that the possession, manufacture and distribution of CSAM (referred to in U.S. legislation as "child pornography") accounts for almost all of Indonesia's reports in the reporting period, as shown in Figure 15.

Reports classified as relating to CSAM ("child pornography") increased by 16% between 2017 and 2019. While the numbers for other types of incidents were comparatively small, and did not increase as rapidly, the presence of several reports concerning suspected offline child exploitation may reflect Indonesia's status as a tourist destination of interest to traveling sex offenders.

Nearly 100% of NCMEC CyberTips for Indonesia in the period 2017 to 2019 came from electronic service providers (i.e., technology companies). A total of 58 electronic service providers submitted at least one report of suspected child exploitation for Indonesia. This would indicate some diversity in the platforms used by the general population, and by OCSEA offenders. Data for the 21 platforms submitting the largest number of reports in 2019 are shown in Figure 16.

Figure 15: CyberTips concerning suspected child sexual exploitation in Indonesia, by incident type.

Incident Type	2017	2018	2019
CSAM, including possession, manufacture and distribution (NCMEC classification: child pornography)[77,78]	727,437	1,223,934	840,191
Travelling child sex offenders (NCMEC classification: child sex tourism)[79]	9	3	1
Child sex trafficking	4	4	7
Child sexual molestation	3	10	2
Misleading domain name	1		
Misleading words or digital images on the internet	4	4	4
Online enticement of children for sexual acts	34	14	16
Unsolicited obscene material sent to a child	2	3	
Total	**727,494**	**1,223,972**	**840,221**

Base: CyberTip data provided by NCMEC.

---

77. The terminology used in this column reflects classification by the National Center for Missing and Exploited Children in line with U.S. legislation. D*isrupting Harm* advocates use of the term Child Sexual Abuse Material, in line with the Luxembourg Guidelines.
78. CyberTips under this category may reference more than one file of CSAM. For example, some reporting electronic service providers include more files per report, as opposed to one image per report and multiple reports per suspect.
79. The terminology used in this column reflects classification by the National Center for Missing and Exploited Children in line with U.S. legislation. *Disrupting Harm* advocates use of the term Travelling Child Sex Offences, in line with the Luxembourg Guidelines.

Figure 16: CyberTips concerning suspected child sexual exploitation in Indonesia, by reporting electronic service provider.

Reporting Electronic Service Provider	2017	2018	2019
Facebook	680,669	1,145,938	756,084
Instagram, Inc	34,683	56,225	57,675
Google	7,492	16,837	22,161
Twitter, Inc/Vine.co	2,337	2,220	1,835
WhatsApp Inc.	128	562	1,145
Pinterest Inc.	305	437	431
MeetMe.com (fka my Yearbook.com)	217	187	190
Imgur, LLC	39	8	91
Dropbox. Inc	85	75	73
sendvid	41	117	59
Tagged.com	40	29	49
Discord Inc.			46
Snapchat	3	9	45
Microsoft online operations	66	70	43
SmugMug Flickr		58	39
Tumblr	109	18	39
Yahoo! Inc	104	48	39
Adobe systems Incorporated	5	6	27
Hacker Factor	48	36	20
Tinder Inc			16
Word press.com/Automatic	2	6	16

Base: CyberTip data provided by NCMEC, sorted by 2019 counts, null results removed.

Facebook was responsible for 90% of the CyberTipline reports made in 2019, and 93% for the reporting period as a whole. The increase of 11% for Facebook reports related to Indonesia between 2017 and 2019 is broadly similar to the trend observed in Indonesia's total NCMEC CyberTips. Although in smaller volumes, there were notable increases between 2017 and 2019 in CyberTipline reports from Google (196%), Instagram (66%) and WhatsApp (795%). Reports from Twitter declined slightly.

Indonesia is unique for the variety of different social platforms, image hosting and video sharing service providers that made reports to NCMEC in 2017-2019. The variety of platforms among the reporting electronic service providers may also speak to the nature of suspected OCSEA offending. Noted were multiple reports from self-avowed "moral-free file host" Motherless.com, anonymous image-based bulletin board 4chan, anonymous social media app Whisper, privacy-focused social media platform MeWe, digital forensics research company Hacker Factor and dark web and peer-to-peer monitoring firm Tiversa. Reports from Discord (46 reports in 2019) and Twitch, often used to facilitate gaming chat and streaming, may reflect Indonesia's adoption of tools and apps that require greater bandwidth.

Figure 17: NCMEC CyberTips concerning suspected child sexual exploitation in Indonesia, number of unique upload IP addresses by year.

	2017	2018	2019	% Change 2017 to 2019	% Change 2018 to 2019
Indonesia unique upload IP addresses	195,283	298,996	299,303	53%	0%
Total Indonesia reports	727,494	1,223,972	840,221	15%	-31%
Reports per unique IP address	3.73	4.09	2.81	-25%	-31%

Base: Data provided by NCMEC. Note that the same IP address may be counted in more than one year.

Multiple reports from Tagged.com, skout.com (44 in total), Match, Tinder and Initech/Growlr speak to the misuse of over-18 dating sites for suspected distribution of CSAM. The reports from Chaturbate, a platform specialising in the provision of adult live-streamed sexual activity that is often paid for in tokens, raises the possibility of OCSEA with a commercial element. Reports from randomised video chat service Omegle and live video broadcast platform YouNow suggest at least some level of engagement with live-streamed CSEA.

Number of IP addresses reported: The NCMEC data for Indonesia also permits analysis of headline statistics for unique Internet Protocol (IP) addresses used to engage in suspected child exploitation, as shown in Figure 17.

An IP address is assigned to each individual device on a specific network at a specific time. The number of unique IPs resolving to Indonesia increased by 53% in 2018 and remained at the same level in 2019 even though the total number of CyberTips declined. Thus, the average number of reports per unique IP address peaked in 2018.

A lower rate of reports per unique IP address is suggestive of a tendency for offenders (or at least their devices) to upload fewer items of CSAM, on average, in a detected session. However, other explanations are possible. It could reflect an increase in reports that contain more than one upload IP address, perhaps reflecting more than one instance of suspected child sexual exploitation, as would be the case for manual reports that collate multiple events for a single suspect. Another factor is the dynamic assignment of IP addresses by the suspect's telecommunications provider. For instance, if a suspect's internet connection were refreshed by the provider while uploading CSAM to a particular platform, it is possible that more than one IP address would be assigned to that device by the telecommunications provider, and therefore captured by the platform reporting to NCMEC. The ongoing transition from version 4 of the Internet Protocol address system, which in recent years has shared 32-bit IP addresses among a large number of devices by means of carrier grade Network Address Translation, to version 6, which assigns a unique 128-bit address to each device, may also have a bearing here. Scrutiny of the content of the NCMEC CyberTips destined for Indonesia would be required to test these hypotheses.

2.1.3 Evidence of CSAM from other sources

CSAM distribution on peer-to-peer networks

Data on CSAM distribution on peer-to-peer file-sharing networks present a rather different picture. According to the Child Rescue Coalition's Child Protection System, a total of 1,124 Indonesian IP addresses engaged in the distribution or downloading of CSAM were identified between 9 June 2019 and 8 June 2020. Since the system does not monitor all file-sharing networks, this should not be taken to be representative of the sum total of CSAM offending on these platforms.

Figure 18: CSAM distribution and downloading of CSAM on peer-to-peer file-sharing networks in *Disrupting Harm* focus countries in Southeast Asia.

	IP Addresses	Globally Unique Identifiers[80]
Cambodia	1,319	95
Indonesia	**1,124**	**202**
Malaysia	2,754	558
Philippines	1,971	1,446
Thailand	3,049	609
Viet Nam	925	141

Base: Data provided by *Child Rescue Coalition* for the period 9 June 2019 to 8 June 2020

Hosting of CSAM

Indonesia has been identified as a hosting country for images and videos assessed as illegal by International Association of Internet Hotlines (INHOPE)[81] member hotlines contributing to the ICCAM platform as follows:

Figure 19: CSAM hosting in Indonesia, as identified by INHOPE members hotlines using ICCAM.

	2017	2018	2019
Illegal Items	13	16	0
Percentage of Global Total	0.01%	0.01%	0.00%

Base: Data provided by INHOPE

The Internet Watch Foundation actioned the following reports concerning confirmed CSAM hosting in Indonesia:

Figure 20: CSAM hosting in Indonesia, as identified by the Internet Watch Foundation.

	2017	2018	2019
Illegal Items	3	7	0
Percentage of Global Total	0.00%	0.01%	0.00%

Base: Data provided by the Internet Watch Foundation.

Since data pertaining to the ICCAM project is limited to submissions from INHOPE member hotlines, and since the Internet Watch Foundation operates primarily as the United Kingdom's CSAM hotline, this should not be taken as the sum total of CSAM hosting in the country.

CSAM distribution via Twitter

Twitter has analysed three million URLs shared by accounts suspended *globally* in the period 2017–2019 for violation of the platform's CSEA policy. The analysis, which was conducted for *Disrupting Harm*, has found that was OCSEA-related activity on the platform. Twitter shared with *Disrupting Harm* team that some accounts in Indonesia were suspended for CSEA related-activity in the country between the years 2017-2019.

---

80. A Globally Unique Identifier is a 128-bit number created by the Windows operating system or another Windows application to uniquely identify specific components, hardware, software, files, user accounts, database entries and other items.
81. The International Association of Internet Hotlines (INHOPE) is a network of 47 hotlines worldwide that aims to remove CSAM from the internet.

Figure 21: Top 5 domains links shared by Twitter users suspended for CSAM related activity, generic shorteners and social media excluded.

	Thailand	Indonesia	Philippines	All Southeast Asia
1	nudyed.net	path.com	curiouscat.me	curiouscat.me
2	2ch-matome-site.com	wl.gs	8ch.net	socialcam.com
3	socialcam.com	tl.gd	ask.fm	path.com
4	swarmapp.com	kecirit.com	dz4link.com	nudyed.net
5	vine.co	socialcam.com	socialcam.com	2ch-matome-site.com

Base: Data provided by Twitter Trust & Safety Team.

The figure above includes the top five domain links with CSAM related activity in Thailand, Indonesia, the Philippines, and across all of Southeast Asia. Twitter has confirmed that in 2017-2019 a number of users were suspended for suspected CSEA-related activity in Thailand, Indonesia, the Philippines, Malaysia, Cambodia and Vietnam. In terms of the behaviour of the suspended profiles, there was a tendency to move to more private channels such as direct messaging, or more private platforms in order to conceal activities. For activities related to live-streaming that took place on private channels, Skype was the dominant platform.

Web searches

Research was conducted on Google Trends[82] with a view to identifying levels of interest in CSAM in Indonesia as indicated by internet searches on the open web.[83]

A sample of twenty specialised terms selected by the INTERPOL Crimes Against Children team served as keywords and phrases for measuring search interest for CSAM. Queries for the period 1 January 2017 to 31 December 2019 on searches in Indonesia returned a result of 'not enough data' for each of these 20 terms.

Returns of 'not enough data' equate to a zero relative popularity score, indicating a comparatively low level of interest in that term (as opposed to absolute zero search volume) within the geographical and time limits set.[84] When compared to the numbers of global searches for the same terms and searches from other countries in the same time frame, this suggests that specialist CSAM search terms may be used less in Indonesia than in some other countries. While it may also be argued that more sophisticated CSAM searchers are less likely to search on the open web, the relative popularity in other countries of some of the terms in the Interpol sample would suggest that open web searches are still used to discover CSAM.

Individuals in Indonesia looking for CSAM may search in languages other than English. However, the use of local language and slang search terms present a key knowledge gap. With this in mind, there exists an opportunity for the law enforcement authorities to review OCSEA investigations in Indonesia with a view to identifying additional terms and search strings used by offenders.

---

82. Google Trends is a publicly available tool that returns results on the popularity of search terms and strings relative to others within set parameters. Rather than displaying total search volumes, the tool calculates a score (on a range of 1 to 100) based on a search term or string's proportion to all searches on all terms/strings. Data points are divided by total searches in the geographical and time parameters set, to achieve relative popularity. While Google Trends draws on only a sample of Google searches, the dataset is deemed by the company to be representative given the billions of searches processed per day. For more information on data and scoring, see "FAQ about Google Trends data".
83. English language terms were selected because local dialects rendered sporadic results. These universal specialist terms were identified by INTERPOL Crimes Against Children team. In order to maintain uniformity in all DH reports, vernacular terms were not used unless otherwise some terms were provided by the law enforcement.
84. Ramadanti, R. (2020). Telling stories with Google Trends using Pytrends in Python.

Queries were also run for some local terms sourced from the national law enforcement authorities, which included words and phrases referring to commercial sex workers, or sex service provider, and referring to private parts of the body. Some terms appeared to be popular in East Java while others produced results in searches in North Sumatra.

Further research is needed into the use of local terms and dialects in searches for CSAM or OCSEA-related material.

2.1.4 Links to travel and tourism

Data collected by INTERPOL from foreign law enforcement as part of the Disrupting Harm project indicates data around travelling child sex offenders in Indonesia. For example, one law enforcement agency reported 30 instances of travel to Indonesia by national sex offenders between January 2015 and May 2020, in addition to one ongoing investigation. Between 2017 and 2020, the U.S. Angel Watch Center, which monitors convicted child sex offenders with scheduled travel outside of the United States, made 53 referrals to Indonesia, representing just under 5% of the total number of referrals to *Disrupting Harm* focus countries in those years. Ninety-two percent (n = 49) of these referrals resulted in the convicted sex offender being denied entry to Indonesia. This high percentage suggests that there is effective cooperation between U.S. and Indonesian law enforcement authorities in preventing CSEA by travelling sex offenders. It also indicates reasonable coordination between Indonesia's Directorate General of Immigration and the specialised unit on Women and Child Protection which investigates cases of child sexual abuse and exploitation.

> **Analysis of the types of incidents reported to NCMEC reveals that the possession, manufacture and distribution of CSAM accounts for almost all of Indonesia's reports in the reporting period.**

2.2 CHILDREN'S EXPERIENCES OF ONLINE SEXUAL EXPLOITATION AND ABUSE IN INDONESIA

Under the *Disrupting Harm* project, OCSEA was defined specifically to include CSAM, live-streaming of child sexual abuse and online grooming of children for sexual purposes. These concepts are used here to organise and present the results of the *Disrupting Harm* research. At the same time, *Disrupting Harm* recognises that the ways in which children are subjected to OCSEA are far more complex and nuanced. The experiences or offences in question often occur in combination or in sequence. Moreover, as explored in the box "The continuum of online and offline child sexual exploitation and abuse" on page 64, OCSEA does not only occur in the digital environment; digital technology can also be used as a tool to facilitate or record in-person sexual exploitation and abuse.

Because relatively few children said they were subjected to OCSEA, potential grooming and other unwanted experiences online, many of the follow-up questions involve small subsamples. In such cases, when the sample is smaller than 50, absolute numbers are presented instead of percentages to avoid mis-representation of the data.

Recognising that sexual exploitation and abuse of children can happen in many different ways and places, most of the survey questions referred to below allowed for multiple responses, so the proportions and figures presented may add up to over 100%. Finally, differences between age groups, boys and girls, or urban and rural areas are only reported when they are five percentage points or more.

An overview of the survey data on OCSEA

The *Disrupting Harm* household survey of 12–17-year-old internet users measured children's exposure to various manifestations of OCSEA, which will be presented individually below. When taken together, the data reveal that in the past year alone, an estimated 2% of internet-using children aged 12–17 in Indonesia were victims of clear examples of OCSEA. This aggregate statistic encompassed four clear examples of OCSEA experiences *in the year prior to data collection*:

1. Someone offered you money or gifts in return for sexual images or videos.
2. Someone offered you money or gifts online to meet them in person to do something sexual.
3. Someone shared sexual images of you without your consent.
4. Someone threatened or blackmailed you online to engage in sexual activities.

The percentage of children in the household survey in Indonesia who reported that they had experienced clear examples of online sexual exploitation and abuse is relatively low by comparison with other Southeast Asian countries where *Disrupting Harm* data was collected.[85]

As explored in chapter 1, children in Indonesia do demonstrate an ability to assess online risks and over half of the children surveyed knew how to operate online safety features, which could partly explain relatively low incidence figures for OCSEA in Indonesia. Nevertheless, OCSEA may have been under-reported in the household survey for the reasons explained at the beginning of this chapter (privacy concerns, shame or discomfort talking about sex, fear of stigma or self-incrimination, and sampling limitations) (see page 42). This is hard to assess, because *Disrupting Harm* was unable to directly engage with children themselves in some planned research activities, which would have allowed for a further interpretation of these findings and a more comprehensive picture of the issue in Indonesia.

---

85. Thailand (9%); Cambodia (11%); Philippines (20%); Vietnam (1%).

Offering children money or gifts for sexual images or videos

What is online grooming?

Disrupting Harm defines online grooming as engaging a child via technology with the intent of sexually abusing or exploiting the child. This may happen either completely online or through a combination of online and in-person contact.

Online grooming is a complex process which is often fluid and difficult to detect, especially where it involves a slow build of trust between the offender and the child over an extended period of time. The child is often 'prepared' for sexual abuse and made to engage in sexual acts online or in person by means of deceit, coercion or threats. However, online grooming can also be abrupt, with an offender suddenly requesting or pressuring a child to share sexual content of themselves or to engage in sexual acts, including via extortion.

The offer of money or gifts to a child in return for sexual images or videos constitutes evidence of grooming with the aim of obtaining CSAM. Among the internet-using children surveyed, 1% (nine children) said that someone had offered them money or gifts in return for sexual images or videos within the past year. There were no clear differences by age group, gender or urban/rural location.

I WAS OFFERED MONEY OR GIFTS IN RETURN FOR SEXUAL IMAGES OR VIDEOS 1% (9)

1%

Base: Internet-using children aged 12–17 in Indonesia from the Disrupting Harm study. n = 995.

Offering children money or gifts for sexual acts in person

It is clear from the conversations with survivors of OCSEA conducted as part of the research for *Disrupting Harm* that the grooming of children online for the purpose of meeting in person to engage in sexual activities is a real threat. Data provided by NCMEC on CyberTips concerning suspected child sexual exploitation in Indonesia shows that a number of reports related to online enticement of children for sexual acts (64 in the reporting period 2017–2019).

Conversations with OCSEA survivors from Southeast Asia

While not necessarily representative of the Indonesian context, conversations held with young people exposed to OCSEA in various *Disrupting Harm* countries in Southeast Asia showed that money was offered as part of the process of grooming a child, especially where there was an intention to meet. In Cambodia, some children were exploited through the offer of money to engage in sexual acts with another person, usually someone not known to them: *"Played messenger chat with each other normally for about a few days. Later, he chatted to me. He said do you want to go and have sex with others for money?"* (RA5-CA-12). Within these accounts there was also evidence of young people being offered money to have sexual pictures of them taken, *"He took photos when I was swimming, swimming with my friends. We swam. He rode a bicycle and took photos, rode a bicycle taking photos. He took photos, we didn't know, he took photos, we'd never heard of that. He finished taking photos, gave me money and then rode away"* (RA5-CA-03).

In the household survey in Indonesia, 1% of the children surveyed said that, within the past year, someone had offered them money or gifts to meet in person to do something sexual (13 children). Younger children aged 12–13 were as likely as older children aged 16–17 to receive these offers. No differences were observed by gender or by urban/rural location. Like other findings, these numbers may be under-reported as children may not feel comfortable or safe enough to disclose their experiences of abuse and exploitation.

I WAS OFFERED MONEY OR GIFTS TO MEET THEM IN PERSON TO DO SOMETHING SEXUAL 1% (13)

1%

Base: Internet-using children aged 12–17 in Indonesia from the Disrupting Harm study. n = 995.

Sexual extortion

Sexual extortion is sometimes used in the grooming process. Once offenders have already obtained sexual images or videos of children through deceit or coercion, they can then threaten to make those images publicly available or share them with the child's friends or members of their families as a way of pressuring the children into sharing more images or engaging in other kinds of sexual activities. Such threats can also be used to extort money. Indonesia does not have legislation regarding sexual extortion, a legal loophole that leaves victims of this crime unprotected.

In the household survey, internet-using children in Indonesia were asked if anybody had "threatened or blackmailed you to engage in sexual activities" within the past year. One percent (12 children) said 'Yes'. Another 2% of children did not answer the question, which may indicate under-reporting due to the sensitive nature of the question. The children were not asked what kinds of threats were used, so it is not clear, for example, whether previously-obtained sexual images were used to extort money or to pressure the children to engage in further sexual activities.

Conversations with OCSEA survivors from Southeast Asia

A conversation with a young survivor from Cambodia clearly illustrates how threats can be used to extort further sexual activity, *"So he shared all my information. He screenshotted all my friends, and after that, he tried to require photos of me. After he required photos of me, I said I wouldn't send any. No, no way. That's when he started to use threats. He screenshotted my whole friends list. He said if he I don't send photos to him, all the friends on my list would get all the photos he had received."* (RA5-CA-07).

SOMEONE THREATENED OR BLACKMAILED ME TO ENGAGE IN SEXUAL ACTIVITIES 1% (12)

1%

Base: Internet-using children aged 12–17 in Indonesia from the Disrupting Harm study. n = 995

Legislation on CSAM and livestreaming

Indonesia's Law on Pornography defines pornography as "sexuality material produced by human in a form of picture, sketch, illustration, photo, writing, sound, audio, motion picture, animation, cartoon, lyrics, body movements, or other communication messages through various media communication and/or performance in public, which include indecency or sexual exploitation which is against social morality".[86] This definition was challenged in 2010 on the grounds that it was too broad, targeted cultural and traditional performances and discriminated against women, but the Constitutional Court ruled that the definition was clear and did not violate the Constitution.[87] On the basis of the definition of "pornography", CSAM is defined as "all kind of pornography that involve the child or include an adult who act like a child."[88] Therefore, Indonesian legislation explicitly covers visual, audio and written material, and potentially criminalises digitally-generated CSAM, including realistic images of non-existent children.

The Law on Pornography comprehensively criminalises acts associated with pornography in general, including CSAM. Prohibited acts include the production, distribution, broadcasting, import, export, offering, sale or purchase, renting or provision of pornography, including CSAM.[89] The law further criminalises obtaining access to CSAM by prohibiting any person from lending or downloading pornographic material.[90] It also makes the viewing and mere possession of CSAM, with no intent to distribute, offences.[91] Law no. 11 of 2008 on Electronic Information and Transactions, further prohibits any person to distribute, transmit or make accessible "electronic information or electronic documents" containing child sexual abuse.[92]

Knowingly attending pornographic performances involving children is not explicitly criminalised under Indonesian legislation. This is also the case when these performances are live-streamed. The only reference to pornographic performances is made in the Law on Pornography, which prohibits any person from "using other people as models for pornographic content"[93] and "showing themselves or other people in performances or in front of public that describes nakedness, sexual exploitation, sexual intercourse, or other that contains pornography elements".[94]

Data from NCMEC's CyberTipline presented in chapter 2.1 show that the possession, manufacture and distribution of CSAM accounted for almost all of Indonesia's NCMEC CyberTips in 2017–2019.

Moreover, 1% of the internet-using children aged 12–17 in Indonesia who took part in the *Disrupting Harm* household survey (11 children) stated that someone had shared sexual images of them without their permission, with no notable variations by gender. Children aged 16–17 were twice as likely than children aged 12–13 to say this had happened to them in the past year. As for other OCSEA-related offences, the number may be under-reported.

86. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, elucidation of Section 1(1).
87. Vaswani, K. (2010). Indonesia upholds anti-pornography bill. Jakarta: BBC News.
88. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, elucidation of Section 4(1)(f).
89. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Articles 4(1) and 29.
90. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Articles 5 and 31.
91. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Articles 6 and 32.
92. Government of Indonesia. (2008). Law No. 11 on Electronic Information and Transactions, Articles 27 and 52 (1).
93. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Article 9.
94. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Article 10.

Treating Child Sexual Abuse Materials under Anti-Pornography Laws

Indonesian law has an all-encompassing ban on all pornography. The law considers child sexual abuse material as a type of pornography, but no dedicated provisions exist in Indonesia that explicitly define 'child sexual abuse material' nor that criminalise the production, distribution, possession, exchange, sale, etc. of it. Therefore, Indonesian laws don't afford any specific protection to children for this crime.

For pornographic material depicting adults, while the imagery itself may be illegal, the acts depicted are generally not. On the contrary, child sexual abuse material are images, videos, audio and other representations of acts which are themselves also illegal – acts of sexual abuse against a child. These different circumstances require different treatment in law. A recorded act of sexual abuse against a child requires specific legislation and appropriate penalties.

Sexual images of children, particularly those shared online, can be circulated widely and viewed repeatedly all over the world, resulting in a continuous sense of shame and fear of being recognised for the victims. When these images or videos are recordings of severe sexual abuse, the trauma associated with those in-person experiences can be repeatedly reactivated by the sharing of the content.

In the household survey, 74% of children and 76% of caregivers stated that sharing naked images or videos of other people should be illegal.

QUESTION/RESPONSES

SOMEONE SHARED SEXUAL IMAGES OF ME WITHOUT MY CONSENT
1% (11)

1%

Base: Internet-using children aged 12–17 in Indonesia from the Disrupting Harm study. n = 995.

How technological development has influenced OCSEA

The wide availability of faster and cheaper internet access has led to the increasing use of video tools in communications. Video chat and live-streaming tools have rapidly gained popularity and are changing the ways people engage with each other, particularly young people. Live-streaming is increasingly used, both amongst small private groups and for 'broadcasts' to large, public, unknown audiences. In Indonesia, 49% of internet users aged 12–17 watch live-streams at least once a week.

While watching live-streams is often harmless and can have many benefits, the misuse of such tools is creating new ways of perpetrating OCSEA, including the following:

Offenders broadcasting child sexual abuse: Live-streaming tools can be used to transmit sexual abuse of children instantaneously to one or more viewers, so that they can watch it while it is taking place. Remote viewers may even be able to request and direct the abuse, and financial transactions can occur alongside it or even within the same platforms.

Streaming platforms do not retain content shared, only metadata concerning access to their services. This means that when the streaming stops the CSAM vanishes, unless the offender deliberately records it.

Self-generated sexual content involving children: As noted in chapter 1.3.3, the rise in self-generated sexual content, both coerced and non-coerced, live-streamed or recorded, poses complex challenges. Even if the production is non-coerced, this content may still make its way into circulation through sharing without permission or nefarious means, such as hacking. Governments and support services everywhere are grappling with how to address these issues.

Analysis for the following sections include children who experienced any of the four forms of OCSEA described above.

Because children can be blackmailed, threatened, or offered money or gifts to engage in sexual activities entirely in-person (without the involvement of technology), for these forms of abuse, only children who said this happened online – i.e., via social media and/or an online game – are included in subsequent analysis as they would represent cases of OCSEA.

How and where OCSEA happens

Of the 22 children who experienced OCSEA, a majority of children said it happened online – either via social media (nine children) or on an online game (four children). Children who reported OCSEA took place on social media most commonly said this happened on WhatsApp (seven children) or Facebook/Facebook Messenger (three children). Instagram, Snapchat, Twitter, Line were cited in smaller proportions, by one child each.

Another four children reported the last time this happened was in person and five children said this happened some other way.

Some children may have been reluctant to disclose how OCSEA took place, either preferring not to say (four children) or simply saying they 'don't know' how it happened (four children).

Disclosure of OCSEA in Indonesia

Of the 22 children who had experienced one of the clear forms of OCSEA described above, ten did not tell anyone the last time this happened.

Some of the children who did not tell anyone about these experiences did not know where to go or who to tell (five children). Other children feared they had done something wrong and decided not to disclose (five children), or that disclosing would cause trouble for them (three children) or their families (one child). Two children thought no one would believe or understand them while another child did not think the incident was serious enough to report. Barriers to children's reporting and reasons for not disclosing will be explored further in chapter 2.5.

Among children who did disclose an experience of OCSEA, friends were the most common confidant (eight children). Some children also chose to tell a sibling (two children), a male caregiver (two children) or a female caregiver (one child) about their experiences. Two children preferred not to say, and five children did not recall whom they told.

Only two children – both girls – who had been offered money or gifts for sexual images made a formal report, via a helpline. None of the children reported their experiences of OCSEA to the police.

Accepting Money or Gifts in Exchange for Sexual Images or Videos

As explored in the context of grooming, children are sometimes offered money or gifts in return for sexual content. The following paragraphs consider the *acceptance* of money or gifts by children in return for sexual content, regardless of how the process was initiated.

While the practice of accepting money or gifts in exchange for sexual activities is not new,[95,96] the use of digital technologies – including by children and young people – to self-produce and send images or videos of oneself in return for money or other material incentives is an emerging trend. This practice could increase the risk of sharing without permission: 90% of the 'youth-generated' sexual images and videos assessed in a study by the Internet Watch Foundation and Microsoft were 'harvested' from the original upload location and redistributed on third party websites.[97]

Given the sensitivity of this topic, only the 15–17-year-old respondents in the household survey were asked whether they had accepted money or gifts in exchange for sexual images or videos of themselves. Among the 530 respondents, less than 1% confirmed that they had done so in the past year. Some children may have been hesitant to reveal their involvement in such activities – even in an anonymised survey – so the true figure could be higher.

95. Surtees, R. (2004). Traditional and Emergent Sex Work in Urban Indonesia. Intersections: Gender, History and Culture in the Asian Context. Issue 10.
96. Hull, T., Sulistyaningsih, E., & Jones, G. (1999). Prostitution in Indonesia: Its History and Evolution. Indonesia: Pusaka Sinar Harapan.
97. Internet Watch Foundation & Microsoft. (2015). Emerging Patterns and Trends Report #1 Online-Produced Sexual Content.

Further research is needed to understand the socio-economic context of children's lives to explain these transactions. In addition to poverty, another factor which may increase children's vulnerability to this form of OCSEA is the widespread availability of digital payment systems including payment by mobile phone. A growing number of children also make use of social media to generate an income, a trend observed in Indonesia. A 2020 UNICEF study conducted on a non-representative sample of 301 children aged 11–18 using social media in Indonesia (n = 77), Malaysia (n = 127), Cambodia (n = 61) and Thailand (n = 36) showed that Indonesian "children frequently spoke about using social media to generate an income, buying and reselling clothes online, as well as making trinkets and selling them through apps such as Instagram and Facebook."[98] These issues are further examined in chapter 2.4.

Gaps still remain concerning this form of OCSEA. Understanding the intricacies around children's motivations to engage in this practice, their understanding of the risks involved, and how they are first introduced to this practice, are important questions that require further study.

> Talking about sex or sexual acts with someone online was considered 'very risky' by 79% of internet-using children – particularly among girls and older children – and by 91% of their caregivers.

2.2.1 (Potential) online grooming

Indonesian legislation neither defines nor criminalises the online grooming of children for sexual purposes.

Potential grooming – children asked to talk about sex

Additional to the above instances which represent clear OCSEA, children were also asked in the survey if they had been subjected to certain experiences in the past year that *could* be an indication of grooming. Those children who had experienced possible instances of grooming were then asked follow-up questions about *the last time* this happened to them: how they felt, whether it occurred online or offline (or both), who did it to them, and whether they told anyone about it. Recognising that sexual exploitation and abuse of children can happen in many different ways and places, most data points below allow for multiple responses and may therefore add up to over 100%.

When the 995 internet-using children in Indonesia who participated in the household survey were asked whether, within the past year, they had been asked to talk about sex or sexual acts with someone when they did not want to, 2% (23 children) said they had received such unwanted requests. Boys (3%) were more likely to have received such requests than girls (1%), as were children living in urban areas (3%) compared to their rural peers (2%). Nearly 3% of children preferred not to say whether they had received an unwanted request to talk about sex.

Depending on the context, these experiences could imply varying levels of harm for the child. For example, a child being asked to talk about sex by a boyfriend or girlfriend but not wanting to engage at that moment might not face serious harm from this interaction. On the other hand, these experiences could also point to malicious instances of attempted grooming; this is why the figure above is described as an instance of *potential* (versus *actual* or *clear*) grooming. Talking about sex or sexual acts with someone online was considered 'very risky' by 79% of internet-using children – particularly among girls and older children – and by 91% of their caregivers.

---

98. UNICEF East Asia and the Pacific Regional Office and Centre for Justice and Crime Prevention. (2020). Our Lives Online: Use of social media by children and adolescents in East Asia – opportunities, risks and harms. Thailand: UNICEF East Asia and the Pacific Regional Office.

Online or offline? The 23 children who received unwanted requests to talk about sex in the past year were asked if this most recently happened in person, on social media, in an online game, or in some other way. Children were most likely to say this happened in person (nine children), on social media (eight children) or via an online game (three children). For three children, this happened in some other way, while five children preferred not to say or did not know how it happened.

The eight children – all aged 14 and above – who said they most recently received unwanted requests to talk about sex via social media were mainly targeted on Facebook (seven children), WhatsApp (three children) and Twitter (two children). A smaller number of children were contacted on Instagram, YouTube and Live.me. While girls were only contacted on Facebook and WhatsApp, boys were targeted on all six platforms.

The responses captured in this survey question could have included cases of purely offline CSEA, because asking a child to talk about sex can happen entirely in person, without any involvement of technology. If the children complied with the request, they could also have done this without any use of digital technology. In order to ensure the data below capture CSEA with a digital element only, the following data only include the children who said they were more recently targeted via social media and/or online games (11 children), as these would represent instances of OCSEA.

How children felt: Most of the 11 children who received unwanted requests to talk about sex online felt negatively about the experience. A majority of children reported being embarrassed or scared. While girls were more likely to report that they were either unaffected or annoyed by the incident, boys were more likely to cite feelings of embarrassment, fear, guilt and distress.

How children respond: When asked to talk about sex online, one of the 11 children surveyed for *Disrupting Harm* complied with the request while four children refused directly. Other tactics used by the children included ignoring the problem and hoping it would go away, refraining from using the internet for a while, or deleting messages from the other person.

I HAVE BEEN ASKED TO TALK ABOUT SEX OR SEXUAL ACTS WITH SOMEONE WHEN I DID NOT WANT TO
2% (23)

2%

Base: Internet-using children aged 12–17 in Indonesia from the Disrupting Harm study. n = 995.

Potential grooming – children asked to share sexual images or videos
Some offenders have the intention of manipulating children into self-generating and sharing sexual images or videos though digital technologies, whether or not they also intend to meet the child in person. In 2015, amid concern about this issue, the Lanzarote Committee in charge of overseeing implementation of the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Abuse (also known as the 'Lanzarote Committee') issued an opinion regarding this. The Committee recommended that states should extend the crime of grooming for sexual purposes to include "cases when the sexual abuse is not the result of a meeting in person but is committed online."[99]

---

99. Council of Europe's Lanzarote Committee. (2015). Opinion on Article 23 of the Lanzarote Convention and its explanatory note. Paragraph 20.

The children who took part in the household survey were asked whether, in the past year, they had received a request "for a photo or video showing their private parts when they did not want to." While these data could capture requests from partners or peers, they could also point to attempts to manipulate children into self-generating and sharing sexual images or videos through digital technologies. Within the past year, 1% of the internet-using children surveyed in Indonesia – mostly older children aged 16–17 and girls – had received unwanted requests for a photo or video showing their private parts (12 children).

How children felt: Most of the children who received these requests felt angry or embarrassed. A few boys felt guilty or betrayed. Only two girls (no boys) reported not being affected by the incident at all.

How children respond: The majority of children did not comply with the request. Most said 'No' but some resorted to less direct tactics such as ignoring the request, changing their privacy settings or deleting messages from the person concerned. Two children did as the person asked.

Online or offline? The children who had received these requests generally said that it happened on social media or in some other way (four children each). The next most likely channels were in-person offers and online games (2 children each).

Of the four children who were approached on social media, one child (a girl aged 16-17) named Facebook, while two boys cited YouTube and WhatsApp as the platforms concerned. One child preferred not to mention the platform on which this occurred.

Offenders and disclosure of online grooming in Indonesia

Who were the offenders?
Children were more likely to receive requests to talk about sex online or to share sexual content from someone already known to them. A romantic partner was cited by five of the 12 children who had received a request to share sexual content and one of the 11 children who were asked to talk about sex online. Requests to talk about sex online came from family members in the case of five children. Friends or acquaintances under 18 were cited by three children in the case of requests to talk about sex and adult friends by one child for each of these *potential* grooming forms.

Of the children who said that they had received unwanted requests to talk about sex online, five children said these came from someone they did not know prior to the incident. A stranger was also cited by three children who were asked to share sexual content. Two other children said they do not know, and one preferred not to say who the offender was.
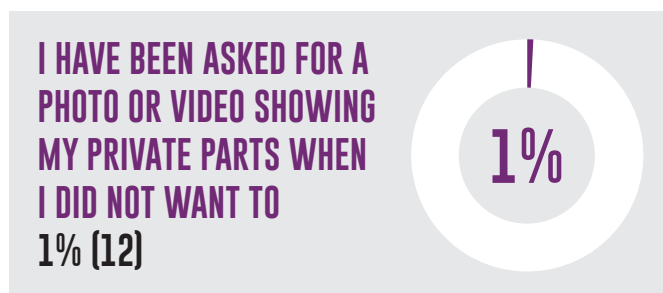
Whom children told?
Many children who were asked online to either talk about sex or to share sexual images and/or videos did not tell anyone the last time this happened. Over half of the children (six children) – all boys – who received a request to talk about sex in the last year did not tell anyone about the incident. Four of the 12 children who had received an unwanted request to share sexual images of themselves when they did not want to within the past year did not tell anyone the last time this happened. Girls and older children were the most likely to keep the incident to themselves. This is very similar to the findings from the conversations with survivors of OCSEA from other countries in Southeast Asia. One young person from Cambodia told how, *"... there's not really anyone who knows. I haven't even told my friends"* (RA5-CA-07).

Six of the 12 children who had been asked to share sexual content online told a friend. Among children who told someone about being asked to talk about sex online, all girls confided in friends while some boys chose to disclose to a female caregiver. Among remaining children who disclose being asked for sexual content online, one told a sibling, and another told a male caregiver.

None of the children made a formal report to the police, a social worker or to a helpline. None of the children who received unwanted requests to talk about sex or sexual acts reported what had happened to them through an online reporting function. This could be because children do not know where to find these mechanisms: of the full sample of 995 children, half (49%) did not know how to report harmful content on social media, while 62% said they did not know where to get help if they or a friend were subjected to sexual harassment or abuse. Almost all the children who most recently received the requests on social media said they were targeted on Facebook or Facebook Messenger (97%). A relatively much smaller proportion of requests were received on platforms like Instagram (11%) or TikTok (9%).

Barriers to children's reporting and reasons for not disclosing will be explored further in chapter 2.5.

> " Many children who were asked online to either talk about sex or to share sexual images and/or videos did not tell anyone the last time this happened… None of the children made a formal report to the police, a social worker or to a helpline. "

I HAVE BEEN ASKED FOR A PHOTO OR VIDEO SHOWING MY PRIVATE PARTS WHEN I DID NOT WANT TO
1% (12)

1%

Base: Internet-using children aged 12– 17 in Indonesia from the Disrupting Harm study. n = 995.

2.3 OTHER EXPERIENCES OF CHILDREN THAT MAY BE LINKED TO ONLINE SEXUAL EXPLOITATION AND ABUSE

In addition to the examples of OCSEA already presented, children may be subject to other experiences online which can be harmful, such as sexual harassment or unwanted exposure to sexualised content. Moreover, these experiences could, in some instances, contribute to the desensitisation of children so that they become more likely to engage in sexual talk or sexual acts – for example, during a grooming process.

Sexual harassment

The household survey showed that 7% of internet-using children (72 children) in Indonesia had, within the past year, been exposed to sexual comments about them that made them feel uncomfortable, such as jokes, stories or comments about their bodies, appearance or sexual activities. Older children were three times as likely to have experienced this (12–13: 4%; 16–17: 10%). No differences between the genders were observed in the statistics.

How children felt: Among the children who had been harassed in this way, one in five said this experience did not affect them, but the majority felt negatively about it. Twenty-six percent said they were embarrassed and 14% annoyed. Smaller proportions of children reported feeling guilty or angry. A few children – all boys – were distressed or scared. Nearly 10% preferred not to say how they felt.

Online or offline? The sexual comments to which the 72 children were subjected were most likely to have been made in person (26%) or on social media (also 26%). Other children were harassed via an online game (10%). One in five said they did not know how the comment was made and one in eight preferred not to say.

Among the 19 children who were targeted *on social media*, Facebook and WhatsApp were the platforms where this most commonly occurred. Twitter, TikTok and YouTube were cited by smaller proportions of children. Twitch, Telegram and Live.me were cited by one child each. While girls were targeted through a limited number of platforms (and most often on Facebook), boys received these sexual comments via a number of different platforms.

Who harasses children? Persons known to the children were most commonly responsible for making discomforting sexual comments. The 72 children most often mentioned adult friends (22%) as the offenders, followed by family members (21%), friends younger than 18 (14%), and romantic partners (7%). Nearly a third of the children had received these sexual comments from someone unknown to them: some did not know who the person was (21%) while others said they did not know the person prior to the incident (8%).

Whom children tell – if anyone: Most of the children who had received discomforting sexual comments in the past year disclosed the incident to someone. Friends were easily the most likely confidant (39%), followed by a female caregiver (8%), a sibling (7%), a male caregiver (3%) or another trusted adult (3%). None of the children reported to the police, a social worker or a helpline. A third of the children did not tell anyone the last time this happened. Boys and older children were the most likely to have kept the matter to themselves.

IN THE PAST YEAR
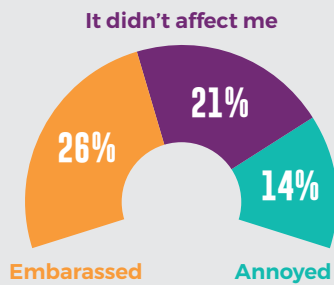# SOMEONE MADE SEXUAL COMMENTS ABOUT ME THAT MADE ME FEEL UNCOMFORTABLE

YES 7% (72)

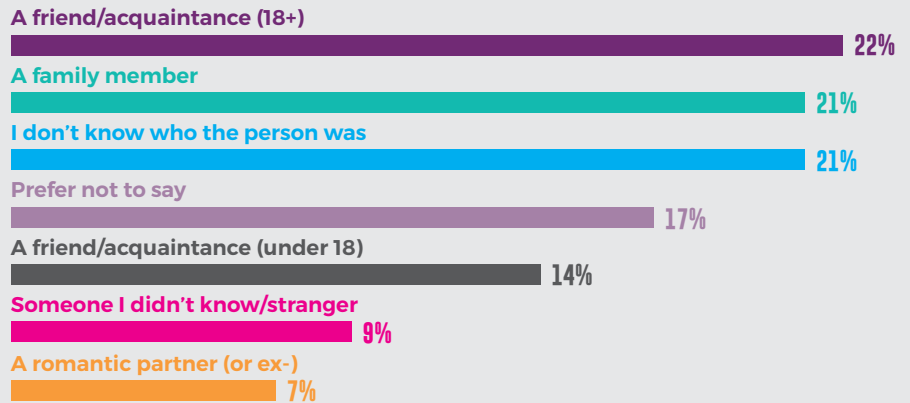Base: Internet using children 12–17
n = 995 children

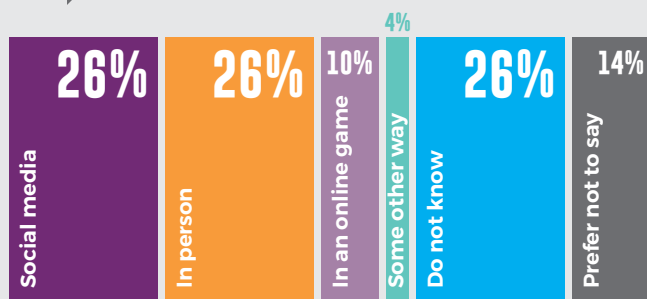## THE LAST TIME THIS HAPPENED...

How did you feel?*

- It didn't affect me **21%**
- Embarassed **26%**
- Annoyed **14%**

Who did it?*†

A friend/acquaintance (18+)	22%
A family member	21%
I don't know who the person was	21%
Prefer not to say	17%
A friend/acquaintance (under 18)	14%
Someone I didn't know/stranger	9%
A romantic partner (or ex-)	7%

Children who experienced sexual comments about them that made them feel uncomfortable. n = 72.

Where did it happen?*†

Social media	In person	In an online game	Some other way	Do not know	Prefer not to say
26%	26%	10%	4%	26%	14%

Children who experienced sexual comments about them that made them feel uncomfortable. n = 72.

Whom did you tell?**†
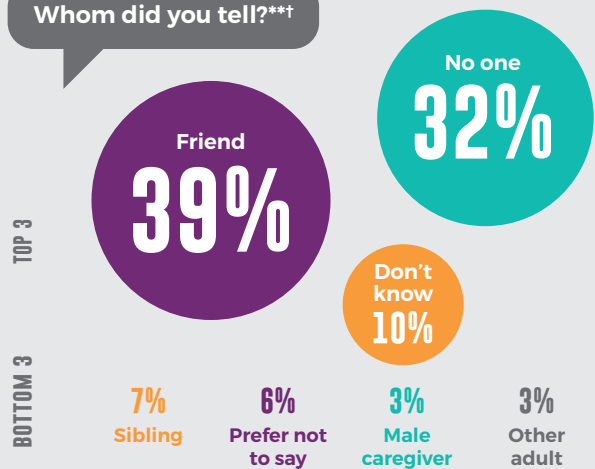
TOP 3
- Friend **39%**
- No one **32%**
- Don't know **10%**

BOTTOM 3
- Sibling **7%**
- Prefer not to say **6%**
- Male caregiver **3%**
- Other adult **3%**

Children who experienced sexual comments about them that made them feel uncomfortable. n = 72.

*These figures represent the most common responses selected by children.
**These figures represent the most and least common responses selected by children.
†Multiple choice question

Source: Disrupting Harm data

2.3 OTHER EXPERIENCES OF CHILDREN THAT MAY BE LINKED TO ONLINE SEXUAL EXPLOITATION AND ABUSE

Receiving unwanted sexual images

A study on Digital Citizenship Safety Among Children and Adolescents conducted in 2015 on a sample of 400 children and adolescents aged 10–19 in Indonesia indicated that while 52% of the respondents had seen pornographic content – either in the form of text, image, photographs or videos– many had come across such content accidentally, including after having opened a link sent to them via email.[100]

Previous research indicates that exposure to unwanted sexual content, including unsolicited images or videos is one of the primary concerns of internet-using children. In a 2020 study involving 301 children between the ages of 11 to 18 in Malaysia, Thailand, Indonesia and Cambodia, 52% of those surveyed had been a recipient of a sexual message, image or video that they did not want.[101]

Among the children surveyed for *Disrupting Harm,* only six percent (64 children) said that someone had sent them unwanted sexual images or videos in the past year. This was somewhat more common for older children. More children in urban areas received such content than those living in rural areas (9% versus 4%). Of the 64 children, 67% said they felt negatively about receiving these kinds of images, while 27% were not affected at all and 10% did not want to answer the question.

> **Among the 35 children who had received unwanted sexual content on social media, 20 cited WhatsApp and another 18 Facebook as the platforms where this most recently occurred.**

Online or offline? Over half of the 64 children who had received unwanted sexual content in the past year said this happened on social media (55%). For other children, this happened in person (20%), or in some other way (8%). Five percent of the children were sent such content via an online game. About one in ten did not know how the content was sent or preferred not to say.

Among the 35 children who had received unwanted sexual content *on social media*, 20 cited WhatsApp and another 18 Facebook as the platforms where this most recently occurred. Smaller numbers named Instagram, Twitter, TikTok and YouTube. Telegram was cited by three girls aged 16–17.

Who sends unwanted sexual content? A majority of the 64 children received unwanted sexual content from someone they know. The offender was most commonly an adult friend (28%), followed by a peer younger than 18 (25%). A family member was responsible in the case of four children, while a romantic partner was cited by two. As many as 29 children said they had received such content from someone unknown to them.

Whom children tell – if anyone: Among the 64 children, 37% (23 children) did not tell anyone the last time they received unwanted sexual content. Boys and younger children (12–13) were less likely to disclose than girls and older children (16–17). Of the children who did disclose the incident, 41% turned to a friend. A few children told a female caregiver (10%), a sibling (6%), a male caregiver (5%) or another trusted adult (3%). One child (a girl aged 14–15) told the police. This was the only case of a child respondent to the household survey who had reported any of the negative online experiences explored in the survey to the police.

100. Gayatri, G. et al. (2015). Digital citizenship safety among children and adolescents in Indonesia. (Perlindungan pengguna media digital di kalangan anak dan remaja di Indonesia). Research and Development Agency for Human Resource, Ministry of Communication and Information.
101. UNICEF East Asia and the Pacific Regional Office and Centre for Justice and Crime Prevention. (2020). Our Lives Online: Use of social media by children and adolescents in East Asia – opportunities, risks and harms. Thailand: UNICEF East Asia and the Pacific Regional Office.

IN THE PAST YEAR
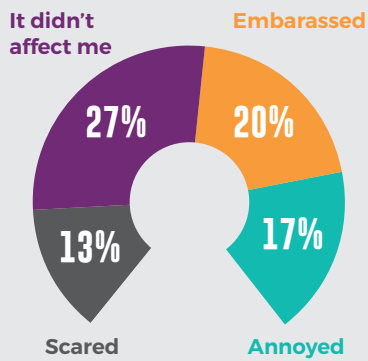# SOMEONE SENT ME SEXUAL IMAGES I DID NOT WANT

YES 6% (64)

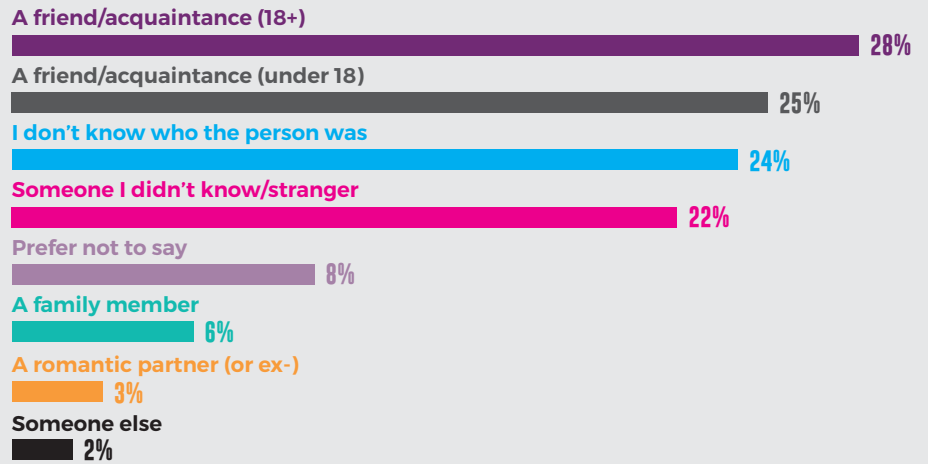Base: Internet using children 12–17
n = 995 children

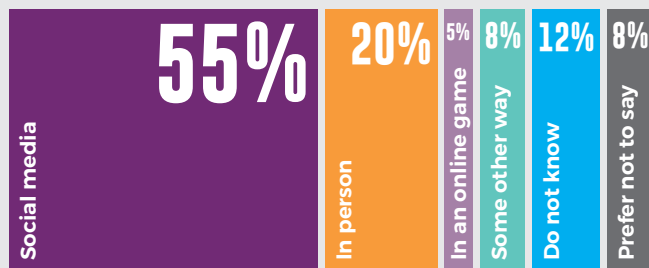## THE LAST TIME THIS HAPPENED...

How did you feel?*

It didn't affect me **27%**
Embarassed **20%**
Scared **13%**
Annoyed **17%**

Who did it?*†

A friend/acquaintance (18+)	28%
A friend/acquaintance (under 18)	25%
I don't know who the person was	24%
Someone I didn't know/stranger	22%
Prefer not to say	8%
A family member	6%
A romantic partner (or ex-)	3%
Someone else	2%

Children who experienced sexual comments about them that made them feel uncomfortable. n = 64.

Where did it happen?*†

Social media **55%**
In person **20%**
In an online game **5%**
Some other way **8%**
Do not know **12%**
Prefer not to say **8%**

Children who experienced sexual comments about them that made them feel uncomfortable. n = 64.

Whom did you tell?**†
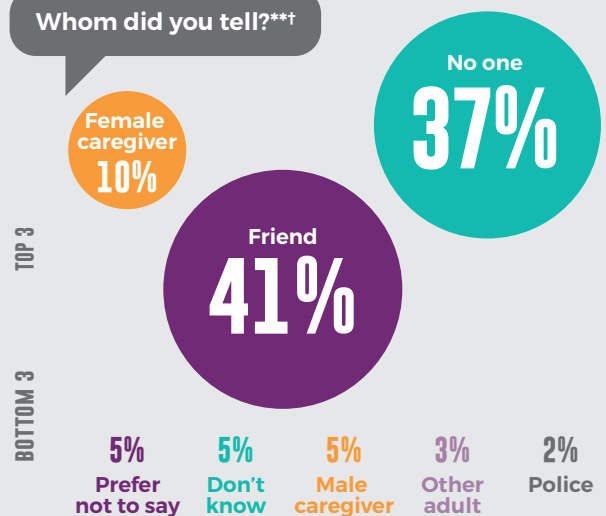
TOP 3

Female caregiver **10%**
Friend **41%**
No one **37%**

BOTTOM 3

Prefer not to say **5%**
Don't know **5%**
Male caregiver **5%**
Other adult **3%**
Police **2%**

Children who experienced sexual comments about them that made them feel uncomfortable. n = 64.

*These figures represent the most common responses selected by children.
**These figures represent the most and least common responses selected by children.
†Multiple choice question

Source: Disrupting Harm data

2.3 OTHER EXPERIENCES OF CHILDREN THAT MAY BE LINKED TO ONLINE SEXUAL EXPLOITATION AND ABUSE

The Continuum of Online and Offline Child Sexual Exploitation and Abuse

The types of sexual exploitation and abuse of children presented throughout this chapter illustrate some of the ways that digital technologies can be used to harm children. However, the research findings also reveal that creating a distinction between online and offline violence does not always reflect the reality of children's experiences. For example, children can be asked or coerced to share self-generated sexual images, and this can happen online, or in person but with the involvement of digital technology. In addition, digital technologies can be used as a *facilitator* of sexual exploitation and abuse. For example, social media or instant messaging can be used to convince or coerce children to meet offenders in person, leading to 'offline' child sexual exploitation and abuse. The data in this report include OCSEA that takes place in the online environment, OCSEA that takes place offline but is facilitated by digital technology, and OCSEA that is committed 'offline' and then repeated by sharing it online.

Interviews and survey data gathered from a range of stakeholders spanning government, the legal system and frontline social service workers suggest that systems are not fully adjusted to this reality, and that OCSEA is sometimes perceived as a 'new kind of abuse' that requires an entirely different response. However, when frontline workers were asked to identify the factors that impact children's vulnerability to sexual exploitation more broadly on the one hand and OCSEA on the other, they typically selected several of the same factors including access and exposure to pornography, increased access to technology and internet, and dropping out of school.

One of the respondents noted: *"The vulnerability of children to OCSEA is almost the same [as that of sexual exploitation] because access is made easier by technology, so it becomes a stimulus for the offender, whether actions are carried out online or offline."* (RA3-IN-26-A)

The data from the household survey clearly show that only a small proportion of children are subjected to OCSEA only. Data from across the *Disrupting Harm* countries consistently shows that a proportion of children subjected to OCSEA are also exposed to an instance of in-person sexual, physical, or emotional abuse. This could indicate that OCSEA is an extension of existing abuse already experienced by the child, or that there are a common set of vulnerabilities that make children who experience violence 'offline' more likely to experience violence 'online' as well.

Responses to OCSEA must be embedded within the broader child protection framework and not handled in isolation. This means enabling OCSEA victims to benefit from the same services that exist for other child victims of violence.

Despite this, there however remains a lack of clarity around the responsibilities of various agencies in addressing cases of child exploitation and abuse with an online element. Furthermore, there are cases where online abuse requires a specialised response, for example in law enforcement investigations involving the use of digital forensics. In other instances, a lack of clear laws around OCSEA make it difficult for law enforcement authorities to act and for children to obtain justice through the courts.

2.4 INSIGHTS ON VICTIMS, OFFENDERS AND ENABLERS

2.4.1 Victims

Age and gender of victims

Apart from the household survey data, very little quantitative data was identified by the *Disrupting Harm* team. Indonesia's child helpline TePSA Kemensos did not provide yearly data submissions to Child Helpline International in the reporting period.[102]

Due to the small sample sizes, it is difficult to draw a conclusive profile of victims of OCSEA in Indonesia from the household survey. Overall, the survey suggests that boys and girls are equally likely to be exposed to most forms of OCSEA, and that children in the age groups 12–13, 14–15 and 16–17 are affected quite similarly.

In 2015, an urban school-based study among 1,738 children aged 12–14 (922 females, 816 males) found high rates of child sexual violence (based on a broad definition which included unwanted physical and verbal acts, being shown photographs of sexual acts, and the passing of sexual comments).

Boys reported experiencing higher rates of victimisation (29%) than girls (21%). In addition, 7% of girls and 21% of boys said they had experienced at least one form of sexual violence in the last six months.[103] In Indonesia's most recent global school-based health survey, lower rates of childhood sexual violence were reported, probably because it was defined as forced sexual intercourse only. In this nationally representative survey of 11,110 children and adolescents aged 13–19, boys again reported more sexual violence (5%) than girls (3%).[104]

Factors affecting vulnerability to OCSEA

Figure 22 below shows the perceptions of the front-line workers surveyed for *Disrupting Harm* concerning the factors which increase children's vulnerability to OCSEA. These perceptions are based on subjective interpretations and do not necessarily reflect the views of the *Disrupting Harm* research teams.

Figure 22: Perceptions of front-line workers of factors about the child impacting children's vulnerability to OCSEA.

Access and Exposure to Pornography	98%
Increased access to technology and Internet	96%
Being left behind by parent/guardian who has migrated for work	94%
Dropping out of school	94%
Family violence	92%
The child themselves having to migrate for work	90%
Living and/or working on the street	90%
Community Violence	90%
Extreme poverty	90%
Cultural practices	86%
Gender Norms	80%
Living with one or multiple disabilities	68%
Belonging to an ethnic minority group	54%

Base: Frontline welfare workers. n = 50.

102. Data submissions confirmed by Child Helpline International, November 2020.
103. Bhatla, N. et al. (2015) Are schools safe and gender equal spaces? Findings from a baseline study of school related gender-based violence in five countries in Asia. International Center for Research on Women.
104. Indonesia Ministry of Health, Ministry of Education, World Health Organization, & Centers for Disease Control and Prevention. (2015). Global School-based Health Survey Indonesia. Jakarta, Indonesia: Ministry of Health.

Exposure to pornography and increased access to technology

As can be seen in figure 22, the frontline workers mostly selected *exposure to pornography and increased access to technology and the internet* as factors affecting children's vulnerability to OCSEA. There is a risk that the common inference of causality between watching pornography and becoming a victim of OCSEA may hinder disclosure and/or lead to victim-blaming and consequently to a lack of support for child victims, as they are seen to be complicit in their own harm.

Education: A large majority of the frontline workers (47 out of 50) believed that dropping out of school increases children's vulnerability to OCSEA. In 2018, primary school enrolment rates stood at 93.5% while 1,555,014 children were out-of-school.[105] There are wide disparities of access to higher levels of education by income and location.[106] Lack of formal education – both of children and their caregivers – may increase the likelihood of a child experiencing sexual abuse.[107]

Poverty: Nine in ten frontline workers surveyed as part of *Disrupting Harm* agreed that *poverty* is a contributing factor to children's vulnerability to OCSEA. Compromising children's choices and opportunities, poverty and financial deprivation render children vulnerable to sexual abuse and exploitation.[108] Although Indonesia is categorised as a lower-middle income country, significant poverty and stark inequalities continue to affect children's well-being.[109] Based on 2018 data, approximately 20% of Indonesians remain at risk of falling into poverty.[110,111]

Disadvantaged groups: The great majority of the front-line workers also cited migration, community and family violence and living on the street as factors that would increase a child's vulnerability to OCSEA.

Low level of parental guidance: One frontline worker stated that *"parents are busy ...and ignore the supervision of their child's use of gadgets and the Internet. Hence children access not only school subjects on the Internet but also social media ...without their parents' awareness."* (RA3-IN-40-A) Similar views were expressed in government interviews. Previous research shows that caregivers in Indonesia have a limited understanding about the use of online technology and also lack time to educate their children about its use.[112]

2.4.2 Offenders

In the absence of data from law enforcement authorities, very little could be ascertained about the profiles of OCSEA offenders in Indonesia. However, some information can be gleaned from the *Disrupting Harm* surveys with children and frontline workers.

Household survey (Note that the children were permitted to select more than one response): Consistent with the evidence about violence against children offline, persons already known to the child were responsible for most of the clear examples of OCSEA (see chapter 2.2) disclosed by respondents of the household survey – often an adult friend (ten children) or a peer under 18 years old (six children), and sometimes a family member (four children). A romantic partner was cited as the offender by three children. Strangers previously unknown to the child were involved in the case of one child only. This has significant implications for prevention and awareness raising, as, globally, many activities focus on the threat from strangers rather than people the child already knows. This should also be a consideration for response systems, as it could be much more difficult for victims to seek help if they are emotionally and/or economically dependent on abusers.

105. UNESCO Institute of Statistics database
106. Beger, G. et al. (2012). Indonesian Youth Online: An Exploratory Study of the Indonesian Digital Landscape. UNICEF New York, Division of Communication, Social and Civic Media Section.
107. Widodo, N., Kurniasari, A., Wismayanti, Y. F., Husmiati, Susantyo, B., Astuti, M., & Padmiati (2014). Perlindungan Sosial terhadap Anak Korban Tindak Kekerasan -Child social protection for the victim of sexual violence. Jakarta: Puslitbangkessos, Kemensos RI.
108. Davy, D. (2017). Regional Overview: Sexual Exploitation of Children in Southeast Asia. Bangkok: ECPAT International.
109. Hasan, A. et al. (2013). Early Childhood Education and Development in Poor Villages of Indonesia. Washington D.C.: International Bank for Reconstruction and Development/The World Bank.
110. The World Bank. Country Overview: Indonesia
111. Pratama, B., Sofian, A., & Talerico, C. (2018). Weighting Approaches on Online Sexual Abuse of Children: Cultural Prevention or Crime-Based Enforcement? Udayana Journal of Law and Culture, 2(2), 191-219.
112. ECPAT Indonesia. (2014). The Scope and Magnitude of Online Sexual Abuse of Children in Indonesia.

In cases where children did not know the identity of the offender (seven children), this could indicate a person known or unknown to the child. Another seven children preferred not to say who the offender was.

Frontline workers survey: Frontline workers who had managed cases that involved OCSEA during the past 12 months were asked as to the typical relationship between the offender and the child victim in the OCSEA cases they handled. The offenders were most commonly said to be either strangers (Indonesian nationals) or family friends. Next came community members over 18, other relatives over 18, community members under 18, caregivers, and lastly siblings over 18. One of the frontline workers said that offenders are *"besides friends, also neighbours who already knew the victim well."* (RA3-IN-10-A)

The frontline service providers commonly identified men as offenders and women as facilitators of OCSEA. When asked about the most common relationship between facilitators[113] and victims in the OCSEA cases they handled, they said the facilitators were most commonly strangers, family friends and community members over 18. A minority of participants indicated that caregivers had been facilitators in cases they had worked on.

2.4.3 Use of multiple platforms

As with other spaces children inhabit, social media platforms can be exploited to target children. As presented in chapter 2.1, the overwhelming majority of NCMEC CyberTips related to Indonesia were from Facebook. This was supported by children's own experiences: large proportions of children in the household survey who had experienced OCSEA also reported that the last time this happened, it was on Facebook or Facebook Messenger (see chapter 2.2).

Important proportions of children surveyed also indicated they were last targeted via WhatsApp, a unique finding in *Disrupting Harm*. Of note, both Facebook and WhatsApp are among the most popular platforms globally, which in part explains why many children experience OCSEA on these platforms.

This may also indicate that offenders use Facebook as an entry point and then move victims onto other, more secure platforms such as WhatsApp. WhatsApp uses end-to-end encryption, a privacy safeguard which ensures that the images, videos, written text and live communications are visible only to the sender and recipient. While end-to-end encryption provides important privacy safeguards to children, it can be misused by offenders to conceal illicit crimes and can prevent detection and investigation of abuse by law enforcement. INTERPOL recently adopted a resolution calling on member countries to urge end-to-end encryption providers to take responsibility for designing products and services which are inherently safe for children and ensure they are able to respond to legal requests to provide law enforcement with relevant information.[114]

2.4.4 Role of electronic payments

The Indonesian e-economy is projected to grow from $7.8 billion in 2015 to $78.8 billion in 2025, with the strongest growth in e-commerce (44%) and online media (28%), which would make Indonesia the largest e-economy in South East Asia.[115] Indonesia is reported to be a mobile-first e-economy and, in 2017, 3.1% of Indonesians aged 15+ had a mobile money account (compared to 0.4% in 2014),[116] a lower figure than in other middle-income countries yet higher than other East Asia-Pacific countries (1.3%).[117]

The growing use of digital and mobile payments assists OCSEA offenders by making it possible to make and receive payments, often instantly and/or anonymously. Offenders may further benefit from an established network of money transfer outlets developed to support remittances by migrant Indonesian workers, but which could simplify payments for sexual images or videos and the live-streaming of child sexual abuse. Indonesia has the second largest migrant worker population in the Southeast Asian region (after the Philippines).

---

113. A definition of 'facilitator' was explicitly defined for the survey participants to answer this question as: "individuals or entities whose conduct (behaviour) facilitates or aids and abets the commission of sexual offence against the child (sometimes referred to as 'intermediaries')."
114. The ICPO-INTERPOL General Assembly Resolution No. 9, Safeguarding children against online child sexual exploitation, GA-2021-89-RES-09 (November 2021).
115. KPMG Siddharta Advisory. (2017). Retail payments in Indonesia: Who will drive the cashless revolution? Jakarta, Indonesia: KPMG Siddharta Advisory.
116. The World Bank. (2017). Global Findex Database.
117. The World Bank. (2018). The Little Data Book on Financial Inclusion.

2.5 BARRIERS TO DISCLOSURE AND REPORTING OF ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

Children taking part in the *Disrupting Harm* household survey in Indonesia broadly indicated that they could depend on their interpersonal networks for help if needed. As many as 91% of children 'agreed' or 'strongly agreed' that a member of their family would help them if they had a problem, and 91% said that they could talk to their friends about their problems. Yet in practice, as shown in chapters 2.2 and 2.3, between 17% and 56% of children subjected to various instances of OCSEA or other unwanted experiences on the internet did not disclose to anyone. Those who did so were more likely to confide in a friend or a sibling than in a caregiver or trusted adult. Only one child reported an incident to the police (about receiving unwanted sexual content) and only one child called a helpline (after receiving an offer of money or gifts in exchange for sexual content).

2.5.1 Reasons for not disclosing and/or reporting

Data from the household survey, access to justice interviews with children, survey of frontline workers and interviews with government duty-bearers all indicate that OCSEA might not be reported by either adults or children in Indonesia due to:

Lack of awareness of OCSEA

While based on a limited sub-sample, some of the children surveyed who chose not to tell anyone what had happened to them attributed this to the fear of not being taken seriously, fear that no one would believe them or understand their situation and/or to not thinking the incident serious enough to report (a reason more frequently cited by boys). For instance, a child who had been offered money or gifts for sexual images and two children who had their sexual images shared without permission did not report for fear that no one would understand the situation.

Another child who had been sexually harassed did not know these activities could be reported and thus did not tell anyone. Three children who had received unwanted sexual content did not think it was serious enough to report. This may point to a lack of knowledge of what constitutes OCSEA, and how serious it is, both among children and among the people around them. As was stated by one government representative, it *"is not yet understood by the people or general public that sexual abuse against children can happen online, without the need to meet between the victim and the offender."* (RA1-IN-07-A)

When frontline workers were asked to appraise the awareness of young people, caregivers and the general public about OCSEA in the frontline workers' survey conducted by *Disrupting Harm*, a majority rated awareness of OCSEA among these different groups as either 'poor' or 'fair' as shown in Figure 23 below.

Figure 23. Frontline workers' perceptions of awareness of OCSEA among children, caregivers and the general public.
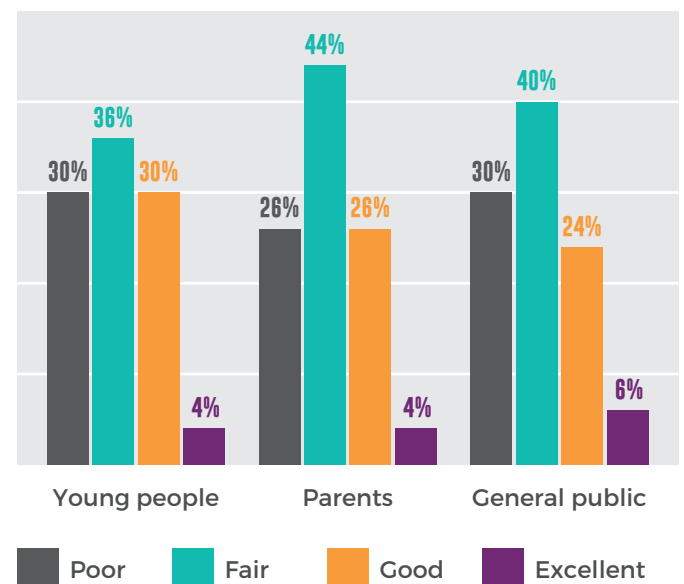
Base: Frontline workers. n = 50.

Interviews with government representatives similarly indicated that public awareness of OCSEA in Indonesia is generally still low. A government representative commented that *"People are rarely aware of OCSEA, even the people with a high educational background."* (RA1-IN-07-A)

Awareness that OCSEA is a crime is important as it provides a basis for initiating legal action. Without this understanding, OCSEA is unlikely to be reported, which is the first step in taking action.

As one frontline worker pointed out, there is a *"lack of public knowledge about OCSEA so that they (the public) cannot determine precisely whether the online content violates the law or not."* (RA3-IN-42-A) Children, their caregivers and the general public need to understand what online actions and online content against children constitute OCSEA if they are to report it.

Caregivers' Knowledge about OCSEA

According to the household survey of internet-using children and their caregivers, caregivers in Indonesia are most likely to obtain information on how to keep their children safe online from family or friends, schools, television and social media (see Figure 24). Five percent of the caregivers surveyed did not get any information about their children's online safety. Friends, family, children's schools and television were the preferred channels through which caregivers said they would like to receive this type of information. While 11% of caregivers said they would like to receive information from religious leaders, in practice none of them did.

The limited public awareness of OCSEA may in part result from a lack of government action on preventing and/or responding to OCSEA. This is described in more detail under chapter 3.4.1.

Figure 24: Caregivers' sources of information on how to support their children's internet use and keep them safe online.

	% who say this is a source of information
Family or friends	65%
Child's school	39%
Television	32%
Social media	21%
Newspapers or brochures	9%
Don't get any information about this	5%
Other sources	2%
Online safety course	1%
Religious leaders	0%
Radio	0%

Base: Caregivers of internet-using children aged 12–17 in the Indonesia. N = 995.

Inadequate knowledge of reporting mechanisms

In the household survey, it was common for children who had experienced OCSEA but had not reported the incident to say that they did not know where to go, or whom to tell. This was the most common reason for non-disclosure among the children who had been asked to talk about sex (four children), that they had received money or gifts in exchange for sexual images (three children), or that sexual images of them had been shared without their permission (one child). This points to insufficient familiarity with reporting mechanisms including helplines, the police and the social media platforms they use. For example, none of the children who received unwanted requests to talk about sex or sexual acts reported what had happened to them through an online reporting function. This could be because children do not know where to find these mechanisms: 48% of the children surveyed did not know how to report harmful content on social media (which could also be because platforms do not signpost these reporting functions well enough or give enough guidance to children about what the reporting process entails), while 62% said they did not know where to get help if they or a friend were subjected to sexual harassment or abuse.

Children in some parts of Indonesia – particularly those in rural areas – may not have access to a helpline. "Not knowing where to go or whom to tell" may also reflect the children's hesitation to tell the people around them for other reasons.

Even if children experiencing OCSEA were to tell their caregivers, the caregivers themselves might not be aware of reporting mechanisms. Asked what course of action they would take if their child was bothered online, only 12% of caregivers said they would report to a helpline, with many preferring to seek help or advice from friends and family (27%).

While 49% of caregivers felt they could help their children cope 'a fair amount' with things that bother them online, close to one in five believed they could not help very much if at all. As 85% of children agree that their caregivers are the persons most responsible for their online safety (after themselves), there is a need not only to equip caregivers with the skills and knowledge to help their children navigate online risks and to respond to online harms they may encounter, but also to consider the role helplines can play as an information resource for caregivers.

Low confidence in the reporting/justice process

Two children who received unwanted sexual content said they did not tell anybody for fear that the incident would not be kept confidential, or that nothing would be done about it. Similar considerations may also affect the likelihood of caregivers making official reports of abuse. When the caregivers who said they would not report harassment or abuse of their children were asked why not, 63% percent cited fears of not being treated properly. Another 20% would not report for fear of repercussions and 11% would not report for fear of negative consequences. Some of these caregivers also showed low confidence in the outcomes, with one in ten believing it would take time and money and that reporting would not change anything.

As *Disrupting Harm* was unable to interview victims of OCSEA and their caregivers who had reported cases and gone through the justice system, further research would be needed to determine whether these beliefs on the part of some children and caregivers are justified.

Shame and stigma

In the household survey, some of the children who did not disclose their experience of OCSEA spoke of a sense of embarrassment or shame or a feeling that it would be emotionally too difficult to tell someone. Embarrassment was the reason cited by one child for not telling anyone about the last time they were asked to send sexual images.

The fact that many children subjected to OCSEA do not tell anyone, particularly an adult, can be attributed in part to common discomfort around openly discussing sex and stigma around sexual experiences. In fact, 41 of the 50 frontline social service providers surveyed believed that stigma from the community influences the reporting of OCSEA in Indonesia. Likewise, 43 of the 50 believed that taboos around discussing sex and sexuality influence the reporting of OCSEA. (see figure 23 above) One frontline worker explained the stigma faced by child victims of OCSEA who have taken the initiative to seek justice as follows: *"On average these children are victims of stigma, for example, when [another] child knows that the child has been victimised and the legal process has run its course and the offender is convicted, this child [victim] will find it difficult to return to school because the stigmatisation process will start in school, from the teacher and so on."* (RA4-IN-05-A-justice) These factors could shed some light on the unusually low numbers of children who reported experiences of OCSEA in the *Disrupting Harm* survey.

Child sexual abuse incidents are considered a disgrace to victims, bringing shame to the family[118] and which many prefer to handle as a private matter.[119] A government representative interviewed for *Disrupting Harm* commented that: *"some parents consider that cases related to sexual abuse as a shame to the family either online and offline case."* (RA1-IN-07-A) A law enforcement representative recalled the reaction he got from an OCSEA victims' family when he visited them; *"They said, 'We are so sorry that you came here because you have exposed our family to shame.'"* (RA1-IN-01-A&B)

For these reasons, both caregivers and children may prefer to keep their experiences of sexual abuse private. In the household survey, when caregivers were asked what course of action they would take if their child was subjected to sexual abuse or exploitation, 54% of caregivers said they would tell a spouse and 34% another family member. In contrast, only 15% would tell a social worker and 13% would call a helpline. Another 54% would – in theory – report to the police. However, as shown in chapter 2.2 and 2.3, children who were subjected to OCSEA in the past year rarely reported the case to law enforcement, helplines, or social workers.

A child abused by an offender of the same sex may have difficulty reporting the offence due to the community stigma associated with homosexuality.[120] In addition to stigma, in one province, religious laws additional to the Penal Code are upheld. Muslim males and females can be penalised for sex outside of marriage or for sex between same-sex partners.[121] In this province, children subjected to abuse by an offender of the same sex may further fear legal consequences if they disclose.

Fear of victim blaming
Children who have experienced OCSEA may feel that they themselves are responsible. In the household survey, 50% of internet using children aged 12 to 17 believed they were the persons most responsible for their online safety. Among children who did not tell anyone about their most recent experience of OCSEA, reasons commonly cited for not disclosing included feeling they had done something wrong or fear of getting into trouble, or of creating trouble for the family. For instance, among the five children who did not tell anyone about their sexual images or videos being shared without permission, three felt they had done something wrong, one child worried about getting into trouble, and another child worried about creating trouble for the family. One child who received money or gifts in exchange for sexual images and another child who exchanged money or gifts for a sexual act also cited a feeling that they had done something wrong as the reason for not telling anyone about the incident.

118. Widodo et al. (2014) cited in: Wismayanti, Y.F. et al. (2019). Child Sexual Abuse in Indonesia: A Systematic review of Literature, Law and Policy. Child Abuse and Neglect, 95.
119. Stark, L. et al. (2018). A qualitative study of community-based child protection mechanisms in Aceh, Indonesia. Vulnerable Children and Youth Studies, 7(3), 228-236.
120. Josenhans, V., Kavenagh, M., Smith, S., & Wekerle, C. (2019). Gender, rights and responsibilities: The need for a global analysis of the sexual exploitation of boys. Child Abuse & Neglect, 110, 6.
121. See e.g., Government of Aceh (2006). Law No. 11 of 2006, Articles 24-33.

Parental attitudes may reinforce these reasons for non-disclosure. Data from the household survey showed that 76% of children and 85% of caregivers believed that it is the victim's fault when a self-generated image or video is shared further. Many children may be unwilling to disclose instances of OCSEA for fear of punishment from their caregivers, including restrictions of their internet use. Indeed, of the caregivers surveyed, 55% stated that if anything bothered their children online, they would restrict their internet use.

It is important to educate the public that experiencing abuse is never the child's fault, and that they should not be punished for it.

Payments made to the victims by offenders

Children who feel as if they consented, at least initially, to their own exploitation may not seek help. Criminal justice professionals interviewed for *Disrupting Harm* further suggested that payments made to child victims for participating in sexual acts make them reluctant to report OCSEA. A representative of the Integrated Service Centre for the Empowerment of Women and Children (P2TP2A) DKI Jakarta, commented that *"When the victim is asked to 'work' and there is consensus/ agreement in the beginning from the child that the child will be paid for the 'work', legally it is child exploitation but from the personal perspective of the child, it is not exploitation."* (RA4-IN-01-A-justice) The Director of the Surabaya Children Crisis Centre stated that: *"Once we reached the Police station to report the child's case, the child was reluctant to report the pimp (…) because the pimp has been feeding and providing the child's daily needs… These cases, in particular, are extremely difficult … due to the child's reluctance to report their pimps. We are forced to delay the case report."* (RA4-IN-02-A-justice)

While, in some circumstances, children may become reliant on the material or financial support they receive from engaging in sexual activities and therefore appear to benefit from these exchanges, it is important to note that children can never consent to their own abuse or exploitation.

2.5.2 Social and cultural influences on reporting of OCSEA

A number of the immediate and underlying factors that prevent the disclosure and reporting of OCSEA appear to have their roots in some wider social factors. Some of these factors could also affect the attitudes of those responsible for the response to OCSEA.

The frontline workers in Indonesia surveyed for *Disrupting Harm* considered taboos surrounding sex and sexuality to be one of the leading social and cultural influences that prevented the reporting of OCSEA, alongside low knowledge of the risks on the part of caregivers (see figure 25).

The frontline workers indicated that there is strong discomfort around discussions of reproductive health, sex and sexuality, and that caregivers avoid discussing these topics with their children. One frontline worker commented that *"if [in] the community [it] is still taboo discussing reproductive health, then children don't have the knowledge, understanding and awareness of the risks of sexual exploitation."* (RA3-IN-36-A) Another frontline worker stated that *"It is very taboo to discuss sex and sexuality in Indonesia, especially when children ask their parents. Most parents will avoid giving answers related to sex and sexuality".* (RA3-IN-40-A) This frontline worker further indicated that due to failure to get information from parents *"children [instead] will find out on the internet or ask people who they think can provide answers such as their girlfriends/boyfriends, their school friends, teachers, or acquaintances they know through social media."* (RA3-IN-40-A)

The household survey indicated that at least 72% of internet using children aged 12–17 had not received any sex education. Among the 20% of children who said they had received sex education, 85% stated that much of the information provided related to morality. Encouragingly, 84% also reported that the sex education they received discussed assertiveness and how to say 'No'.

Figure 25: Social and cultural influences on reporting OCSEA reported by frontline workers.

Category	Percentage
Taboo to discuss sex and sexuality	86%
Low knowledge of the risks from parents	86%
Stigma from community if a known victim	82%
People know it happens but tolerate it	74%
People don't know mechanism for reporting	72%
Low status of children means no rights to report	50%
Cannot trust services to be confidential	48%
Poor quality of service for reporting	44%
Victim is punished	40%
Police don't accept report	34%
Expected roles for men &women	30%
No hotline or helpline	24%
Other	16%

Base: Frontline workers. n = 50.

With regard to sources of sex education, a majority of children (74%) reported that school teachers were the primary source of information, followed by mothers (52%). School teachers were the preferred source of sex education for 28% of children surveyed. As many as 37% of children said they did not want to receive any sex education. This may indicate that children share the belief that sex education is a moral issue or have internalised the social discomfort discussing the topic. Feelings of embarrassment may be shared by caregivers, who have a critical role to play in their children's sex education. Previous research shows that a majority of caregivers feel such conversations are not acceptable in Indonesia.[122] Inability and/or unwillingness to learn about sexuality, including consent and bodily integrity, may seriously hinder reporting of OCSEA and in turn responses to incidents of abuse.

Slightly more attention has been paid to child sexual abuse in the media in recent years, and awareness of it as a serious issue requiring action has increased.[123] However, open discussion of any issue involving sex continues to be hindered by social and religious influences that permeate almost every facet of life in Indonesia.

The legislative sphere has been impacted with the example of non-acceptance of non-heteronormative gender and sexualities leading to recent discussions of a legal change that would have made homosexuality and transgenderism illegal. These moral concerns have not been limited to anti-LGBT responses and have also extended to broader discourse regarding sexuality across Indonesia, for instance, with regard to premarital sexual activity.[124] Such discourse can heighten concerns among the general population and discourage open discussions and age-appropriate sharing of information with young people.

122. Nurachmah, E. et al. (2018). Mother-daughter communication about sexual and reproductive health issues in Singkawang, West Kalimantan, Indonesia. Enfermeria Clinica. Vol28, Issue S1:172-175.
123. Wismayanti, Y.F. et al. (2019). Child Sexual Abuse in Indonesia: A Systematic review of Literature, Law and Policy. Child Abuse and Neglect, 95.
124. Madasari, O. (2021). Shall we Dance? Defining Sexuality and Controlling the Body in Contemporary Indonesia. Religions 12(4): 264

3. RESPONDING TO ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN INDONESIA

This chapter presents evidence on the current Indonesian response mechanisms. This includes formal reporting options, and responses by police and the court system. Finally, it considers the contributions which government, civil society and the internet and technology industry make to combating OCSEA in Indonesia. Much of the data is drawn from qualitative interviews with government, law enforcement and court professionals.

3.1 FORMAL REPORTING MECHANISMS

As seen in the previous chapter, few children report cases of OCSEA to formal reporting mechanisms like the police or helplines. Similarly, some caregivers would also hesitate to report OCSEA to the police. In the household survey of 995 caregivers, 54% said that they would – in theory – tell the police if their child was subjected to sexual harassment, abuse, or exploitation, but others said they would not report due to concerns about negative consequences, fear of not being treated properly and/or the belief that reporting would have no effect. In the frontline workers' survey, 48% said that they believed OCSEA cases are not being reported because services are not trusted. The ability to recognise OCSEA and knowledge about how to report may also affect the level of reporting.

3.1.1 Hotlines, helplines and other government mechanisms

Hotlines and helplines

There are several channels through which children and adults can report cases of OCSEA. These include CSEA hotlines and child helplines. CSEA hotlines focus on working with the industry and law enforcement agencies to take down content, and they now more often use a web-only format rather than phone numbers. The child helplines tend to respond to a broader range of child protection concerns, although some may focus specifically on online child sexual exploitation and abuse. Some helplines provide immediate crisis support, referrals and/or ongoing counselling and case management services.

In Indonesia, the main channels through which children and adults can report cases of OCSEA are the SAPA 129, *Telepon Pelayanan Sosial Anak- TePSA (1-500-771)*, Aduankonten.id, the Integrated Service Centre for the Empowerment of Women and Children, the Indonesia Child Protection Commission and the police.

Child helplines

The SAPA 129 is a national helpline managed by the Ministry of Women Empowerment and Child Protection and operates a toll-free hotline, which aims to assist children who are in emergency situations. This helpline was previously referred to as *Telepon Sahabat Anak* 129 and was said to have ceased national level operations but in 2020, it was reactivated by the Ministry of Women's Empowerment and Child Protection and re-branded as SAPA 129, and can now be accessed nationwide. When an incident is reported to this helpline, a counsellor or case manager links the victim to Unit *Pelaksana Teknis Daerah Perlindungan Perempuan dan Anak* (UPTD PPA) or to a social worker from the Ministry of Social Affairs at the district level. The *Telepon Pelayanan Sosial Anak- TePSA* (1-500-771) is also a helpline for children which aims to protect and ensure the safety and well-being of children in need or in emergency situations.[125] This helpline, just like *Telepon Sahabat Anak* 129, can also be accessed nationwide. For these two helplines there was no information available on the number of OCSEA cases received.

125. O'Kane, C. & Lubis, S. (2016). Alternative Child Care and Deinstitutionalisation: A case study of Indonesia. SOS Children's Villages International & European Commission.

CSAM Hotlines

The Aduankonten.id hotline is run by the Ministry of Communication and Information Technology and allows the public to report content found on websites, social media accounts, mobile applications, and software that violate the 2008 Electronic Information and Transactions Law.[126] Content that can be reported includes child sexual abuse material and violence against children. Links to, and screenshots of, reported sites or content can be uploaded and cases can be monitored while they are being investigated by the Content Complaints team. The Ministry received 60,135 complaints in 2017 compared to 6,357 in 2016. Of these, 19,778 were related to pornographic content and 150 to child abuse. Three websites that featured child abuse were closed down.[127] There is no specific figure for the number of complaints related to OCSEA.

Other reporting mechanisms

OCSEA cases can also be reported through the Integrated Service Centres for the Empowerment of Women and Children (P2TP2A). Government representatives interviewed for *Disrupting Harm* pointed out that the centres have hotlines and WhatsApp numbers that can be used to report OCSEA incidents. Additionally, a representative interviewed from the Indonesia Child Protection Commission also pointed out that the Commission receives *"complaint[s] or report[s] when there is online child sexual abuse"*. Nevertheless, this representative noted that, *"not everyone in the society understands the procedures to file a report or complaint to the Indonesian Child Protection Commission."* (RA1-IN-07-A) No information was however available regarding the number of OCSEA reports made to either the Integrated Service Centres for the Empowerment of Women and Children (P2TP2A) or the Indonesia Child Protection Commission.

3.1.2 Law enforcement agencies

Some government representatives and criminal justice professionals interviewed for *Disrupting Harm* indicated that community members either report OCSEA to the police directly or to civil society organisations which then forward the cases to the police. One government representative pointed out that caregivers are reluctant to report OCSEA cases to law enforcement authorities. (RA1-IN-01-A&B) In the *Disrupting Harm* household survey, 11% of those caregivers who said they would not report their child being sexually harassed, abused, or exploited said they would not report because it would cost time and money. A criminal justice professional representing a civil society organisation commented that: *"when we file a report as an institution to the police, the police will handle the process much faster because they have A-1 (valid) information."* (RA4-IN-04-A-justice)

> **In the *Disrupting Harm* household survey, 11% of those caregivers who said they would not report their child being sexually harassed, abused, or exploited said they would not report because it would cost time and money.**

---

126. Government of Indonesia. (2008). Law No. 11 on Electronic Information and Transactions.
127. Ministry of Communication and Informatics. (2017). Annual Report 2017. Jakarta: Ministry of Communication and Informatics.

3.2 LAW ENFORCEMENT RESPONSE

3.2.1 The enforcers of the law

During the research conducted for *Disrupting Harm*, the Women and Child Protection Unit, the Cybercrime Directorate, its sub-directorates, and the Digital Forensic Unit were mentioned as the law enforcement units within the Indonesian National Police that are most relevant in addressing OCSEA.

Women and Child Protection Unit

The Women and Child Protection Unit is responsible for investigating crimes against women and children in provincial and district level police departments and is often managed by female law enforcement officers who receive training on techniques for interviewing child victims and witnesses.[128] According to a representative of the Unit, *"Our priority is working with policewomen because they have more sensitivity to the issue so it is naturally easier for them to build trust with the victim"*. This respondent however added that there is a *"limitation (…) because of lack of policewomen in our unit."* (RA1-IN-02-A) When handling CSEA cases that have an online component, the Women and Child Protection Unit collaborates with the Cybercrime Directorate. As was pointed out by the representative of the Women and Child Protection Unit: *"If the Women and Children Service Unit needs the back-up from the cybercrime team to investigate the [OCSEA] case, they surely will help us… particularly in providing the evidence regarding its online or cyber aspect of the crime. It requires specific tools and mechanism that is only owned by the Cybercrime Directorate".* (RA1-IN-02-A)

Cybercrime Directorate and its sub-directorates:

The mandate to investigate online crimes, including OCSEA, falls under the Cybercrime Directorate. In the words of a representative from the Cybercrime Directorate: *"When we talk about the case related to online, it is our work at the National Police Headquarters in Cybercrime Directorate and the provincial level of POLDA. We have 34 Cybercrime sub-directorates in regional police all over Indonesia."* (RA1-IN-01-A&B) Government representatives pointed out that the Cybercrime sub-directorates only exist at the provincial level and have no officers at the district level police units. The sub-directorates collaborate with the Women and Child Protection Units in addressing cases that involve children, either as offenders or as victims.

Digital Forensic Unit

The Digital Forensic Unit is the law enforcement unit in Indonesia that receives CyberTips from NCMEC.

It is located in Jakarta and has the technical expertise and equipment for investigating cybercrime, including OCSEA.

- **Staffing:** The Digital Forensic Unit has very few staff to undertake triage and investigation of OCSEA cases for the entire country. There is a large number of referrals from NCMEC. Although detailed information on human resources was not available, a representative of the unit indicated that staff numbers are far too few to handle all the referrals. The law enforcement authorities were said to be cognisant of these challenges and working to address the issue.

- **Capacity and training:** A representative of the unit reported that its team of specialists has the necessary legal knowledge to undertake investigation of OCSEA cases. The Unit uses artificial intelligence enabled tools to undertake investigations. Some of these are FTK (Forensic Toolkit), Cellebrite and Griffeye to triage and analyse any CSAM seized. The unit does not, however, have a 'stand-alone' or exclusive internet connection. None of the unit's equipment is exclusive to OCSEA, as it is also used for other investigations. The team does not work on undercover operations. While officers have participated in regional and international victim identification exercises, specialised training on victim identification was still identified by law enforcement officials as an unmet need. There is broad agreement on the importance of a victim-centred approach, but no child friendly interview facilities are available on the premises of the Digital Forensic Unit.

- **Investigation procedures:** Standard operating procedures are available for conducting investigations, and digital forensics data are stored in the central laboratory on an encrypted server.

---

128. UNICEF. (2016). Child protection in the digital age. National responses to online child sexual abuse and exploitation in ASEAN Member States.

3.2 LAW ENFORCEMENT RESPONSE

Law Enforcement Cooperation with National Stakeholders and Data Access

- *Cooperation with non-governmental organisations*: There is no specific collaboration with non-governmental organisations or health care professionals to support investigation procedures. There is no system for sharing data between the Digital Forensic Unit and non-governmental organisations working on OCSEA.

- *Sharing data with the police and relevant departments:* There is a mechanism to share data on OCSEA between the Digital Forensic Unit and the Cyber Crime Investigation Division.

- *Mechanisms for other government departments to share information:* There is no mechanism for other government departments to share information with the Digital Forensics Unit.

- *Cooperation with financial institutions:* If there is any monetary transaction related to a crime, the Digital Forensic Unit is able to procure information from the bank or financial institution that appears to be involved in that particular case.

Cooperation with the Ministry of Communication and Information Technology: In the words of a representative of the Cybercrime Directorate, *"About cooperation between the Ministry of Communication and Information and National Police Headquarters as law enforcement in terms of exchanging child sexual abuse material or child sexual exploitation material data to be followed up by Indonesia National Police POLRI, I can say that this has not been established yet."* (RA1-IN-01-A&B) This could indicate a significant gap in the investigation process of CSAM cases.

International Law Enforcement Cooperation against OCSEA in Indonesia

- The Digital Forensic Unit works in collaboration with the U.S. Federal Bureau of Investigation and the Homeland Security Investigation department. The respondent from the Digital Forensic Unit said that a seven-member team from the Digital Forensic Unit was enabled to participate in the Dallas Crimes against Children Conference, a large OCSEA-related annual conference, in 2017, and that this was followed by an intensive capacity building exercise by the Federal Bureau of Investigation team in 2018.

- The Virtual Global Taskforce is an international alliance of law enforcement and private sector agencies dedicated to protecting children from online sexual exploitation and abuse. The Indonesian Police joined the task force in 2013,[129] the first police force from the ASEAN region to do so.

- In 2018 the Jakarta Centre for Law Enforcement Cooperation hosted a conference on Transnational Child Sexual Exploitation. The conference also marked the start of cooperation with the Australian police to fight this crime. The police forces committed themselves to working together to raise awareness of transnational online child sexual exploitation and abuse and sexual exploitation of children in the context of travel and tourism.[130]

---

129. EUROPOL. (2013). Dutch, Indonesian, Korean National Police Forces Join Virtual Global Taskforce at European Cybercrime Centre. The Hague, Netherlands: EUROPOL Media & Press.
130. Australian Embassy Indonesia. (2018). Jakarta Centre for Law Enforcement Cooperation Hosts Transnational Child Sexual Exploitation Conference: Media Release.

Promising practices and opportunities

- **Acknowledgement of the issue:** The law enforcement authorities acknowledged the scale and scope of OCSEA during several interactions in an attempt to collect data as well as during the validation meeting with law enforcement authorities. They also acknowledge some of the gaps in the law enforcement response to OCSEA, including an unmet need for specialised training on victim identification following the reconnection with INTERPOL's International Child Sexual Exploitation database; the internal challenges of staff allocation, capacity building, succession planning, and creating a critical pool of investigators in this specialised area of crime.

3.2.2 Gaps and challenges

Government representatives and law enforcement officers interviewed pointed out challenges faced by law enforcement in responding to OCSEA in Indonesia. The challenges and gaps outlined below represent the opinions of the respondents and do not constitute exhaustive evidence.

- **Resources:** Beyond specific issues of staffing and training, some respondents from law enforcement agencies suggested their overall budgets were insufficient. Some felt that the police, as a whole, were not well funded; others that the particular crime area of OCSEA is not a priority for the government and the law enforcement sector. The representative for the Women and Child Protection Unit explained that *"the National Police Headquarters has a limited budget."* (RA1-IN-02-A)

- **Investigative capability:** Although the investigative capabilities of officers have been built through international cooperation, the frequent rotations of police officers and the inability to offer regular, continuous, and specialised training to incoming law enforcement officers hampers the effectiveness of OCSEA training programmes.

- **National Criminal Records:** According to the response of a law enforcement officer, there is no national system to manage sex offenders and no national criminal record registry on this specialised crime area. There is also no system for vetting foreign nationals who come to seek employment in Indonesia.

- **Local capacity:** One government representative interviewed pointed out that law enforcers in the smallest units – for example, at the village level – have limited capacity for handling OCSEA, and that there is therefore an opportunity to empower them. *"We have thousands of officers called Bhabinkamtibnas that work at the village level. Bhabinkamtibnas [local police] also have the mission to do preventive measures in general. However, regarding the OCSEA, we need... an update from time to time because online-based crime is evolving from time to time."* (RA1-IN-01-A&B)

- **Psychosocial support for investigators:** Interviews with law enforcement officers revealed that no mental health or counselling support services were available to the investigation team at the time of the research, despite the fact that viewing of CSAM affects the health and well-being of the officers, who may experience secondary traumatic stress disorder.

> 66
>
> Specialised training on victim identification continued to surface as an unmet need for capacity building by law enforcement.
>
> 99

3.2.3 Step by step: What happens when a child goes to the police?

The interview process:

After receiving a report of OCSEA, the police involve officers from the Women and Child Protection Unit when taking evidence from a child victim, as these officers are trained on interviewing child victims and witnesses.[131] Justice professionals interviewed indicated that information taking is carried out in special interview rooms designed for children. Justice professionals also pointed out that the police sometimes involve non-governmental organisations to provide emotional support to the child during the interview process. A representative from a non-governmental organisation stated that the interview can sometimes be held in a place recommended by a civil society organisation, to avoid the possibility of the child victim meeting the offender. (RA4-IN-04-A-justice) Another justice professional also explained that police officers do not wear uniforms while conducting investigations. (RA4-IN-03-A-justice)

In terms of the uniformity in the application by the police of the above-mentioned child friendly measures, a justice professional indicated that *"This is very varied… when we accompany victims, I can see that there is a difference [in the application of child friendly standards] between the different levels of police stations, from the district-level police station, the city-level police station, and the provincial-level police station, even up to the national policy level."* (RA4-IN-03-A-justice)

Passing the case on to the Children's Court

Interviews with criminal justice professionals revealed that not all OCSEA cases reported to the law enforcement authorities successfully proceed to the prosecution stage. The reasons why cases sometimes do not proceed to prosecution were mentioned as being the withdrawal of the complaint, and challenges in securing the required digital evidence to support the prosecutions.

Withdrawal of complaints: One justice professional commented that withdrawals happen because *"The victims feel intimidated by the offender in certain cases"* (RA4-IN-01-A-justice) while another indicated that *"victims dropped their case due to internal pressure from family members."* (RA4-IN-08-A- justice). Regarding the **challenges in securing digital evidence**, a senior legal advocacy officer from a civil society organisation pointed out that, *"Our law enforcement, when they analyse child sexual abuse cases, they need proof/evidence. This evidence is always the problem… There are plenty of cases where the victims are tired of waiting, … We had a case where…the investigation was halted."* (RA4-IN-06-A- justice) Several factors may be contributing to the challenge of securing digital evidence, which may include a back log of cases which results in delays in the finalisation of investigations, as well as technical challenges.

Despite the challenges cited above, the criminal justice professionals interviewed indicated that most cases filed with the assistance of civil society organisations or other institutions proceed to prosecution.

---

131. UNICEF. (2016). Child protection in the digital age. National responses to online child sexual abuse and exploitation in ASEAN Member States.

3.3 OBTAINING JUSTICE AND ACCESS TO REMEDIES

3.3.1 Court proceedings

Technical capacity of justice staff

A government representative pointed out that the number of law enforcement officers, judges and prosecutors specialising in children's cases is limited when compared to the actual volume of children's cases. (RA1-IN-02-A) Though the mandatory training of criminal justice professionals who specialise in children's cases is a positive point, a government representative (RA1-IN-02-A) was of the view that it is in part also contributing to the small number of justice professionals that specialise in children's cases. Mandatory training of criminal justice professionals specialising in children's cases is carried out as part of the implementation of the Law on the Child Criminal Justice System (*UU Sistem Peradilan Pidana Anak*). Criminal justice professionals are trained on how to implement child friendly procedures when interacting with child victims and witnesses, as part of this mandatory training. Professionals required to undergo this mandatory training include police investigators, prosecutors, judges, probation officers and social workers.[132] A judge from the Supreme Court interviewed for *Disrupting Harm* explained that *"Even before an individual is inaugurated to become a judge [handling cases involving children], they're required to attend a juvenile judge certification and training provided by the Supreme Court."* (RA4-IN-10-A-justice)

Although government representatives indicated that training is provided to justice professionals specialising in children's cases, one criminal justice professional suggested that the application of the knowledge of child-friendly standards is greater among criminal justice professionals in larger cities than among those in more remote areas. (RA4-IN-07-A-justice)

Child-friendly courts

The Law on the Child Criminal Justice System[133] regulates the judicial process for children. Article 18 states that in handling cases involving child victims and/or child witnesses, criminal justice professionals should pay attention to the best interests of the child.[134] The law also provides that the identity of the child must be kept confidential in print or electronic media.[135]

Regarding the implementation of the above provisions, the criminal justice professionals interviewed said that a number of child-friendly measures are observed in OCSEA cases. Proceedings are conducted in juvenile courtrooms and for *"trials involving children and sexual cases, the hearing itself will not be open to the public"*. (RA4-IN-03-A-justice) According to a judge, *"We take off our togas during the investigation and hearing process of the juvenile victim."* (RA4-IN-10-A-justice) With respect to safeguarding the identities of child victims, one justice professional noted that, *"We try to communicate with reporters.... so that photos and names are blurred."* (RA4-IN-03-A-justice)

The use of these measures does not appear to be standard in the more remote regions. In the words of a criminal justice professional, *"Courts in smaller regions don't implement a juvenile court proceeding... a child victim is treated the same as an adult. Moreover, the judges in the more remote regions have a bad perspective toward the child victims."* (RA4-IN-07-A-Justice) This respondent went to explain that: *"In court, the judges must not wear their uniforms or togas [during] juvenile criminal proceedings. I see this procedure has been practiced by courts in Jakarta, but... when we accompanied a child victim to a court located in a smaller region outside of Jakarta, we can see the judges were still wearing their togas and crazily enough the courtroom was open for the public."* (RA4-IN-07-A- justice)

The interviews suggest that child/victim-friendly approaches have not been implemented by all criminal justice professionals.

Duration of process and trial

Interviews with criminal justice professionals revealed that delays in the investigation and trial of OCSEA cases is a major obstacle faced by child victims of OCSEA when seeking justice within the criminal justice system. According to a judge of the Supreme Court, although juvenile cases should only take *"two months, more or less, to determine a judicial verdict ... the process might take longer if the police investigation process is more complicated."* (RA4-IN-10-A-justice)

---

132. Government of Indonesia. (2012). Law No. 11 of 2012 on the Child Criminal Justice System. Article 25 (3), 41 (2), 43 (2), 63 (2).
133. Government of Indonesia (2012). Law No.11 of 2012 on the Child Criminal Justice System.
134. Government of Indonesia (2012). Law No.11 of 2012 on the Child Criminal Justice System, Article 18.
135. Government of Indonesia (2012). Law No.11 of 2012 on the Child Criminal Justice System, Article 19.

Another criminal justice professional commented that *"Due to the lack of manpower as opposed to the ever-increasing number of sexual abuse or exploitation cases, the [investigation and trial process] might take a little longer to complete."* (RA4-IN-08-A-justice) One of the frontline workers surveyed recalled a case in which *"The report was received but the case handling process took very long."* (RA3-IN-14-A) An advocacy lawyer from a civil society network the Anti-Human Trafficking National Network also commented that *"The process of collecting evidence, reporting the case to the police then eventually to the Attorney's office can take a long time which is an exhausting process for the children."* (RA4-IN-07-A-justice)

Legal Aid
The right to legal assistance for children is covered under the Child Protection Law[136] and Article 64 of this law, as amended in 2014, makes the government responsible for providing effective legal assistance.[137] These provisions of the law do not however make specific reference to child victims of abuse and exploitation. Instead, the Child Protection Law specifically states that a child victim be provided with protection and accompaniment during the court process.[138] On 12th April 2022, Indonesia's parliament approved the Sexual Violence Bill,[139] but as the signed and final version of this law was not publicly available during the writing of this report, the research team could not establish if the right to legal assistance for victims of child sexual abuse and exploitation is explicitly covered.

The criminal justice professionals interviewed indicated that some civil society organisations provide legal assistance to child victims of abuse. The organisations mentioned included the Centre for the Study of Child Protection,[140] which has a unit that provides legal assistance to both child victims and child offenders, and the Surabaya Children Crisis Centre, which is an organisation that focuses on legal assistance, advocacy, reintegration and resocialisation before and after the criminal justice process.[141]

3.3.2 Compensation
Under Indonesian law, child victims of child sexual abuse material, sexual exploitation and other sexual crimes have the right to apply to the courts for restitution of damages from the offenders.[142] Children can pursue such restitution either in an independent civil case or in a criminal proceeding.[143] In practice, criminal justice professionals identified some barriers to obtaining compensation.

Failure to apply: Criminal justice professionals sometimes omit to submit an application for restitution to the court. As a representative from the Bahtera Foundation pointed out, to obtain restitution, *"an application must be made."* (RA4-IN-04-A-justice) *"The police, and prosecutors, never apply the restitution clause,"* argued the administrator from the Embun Pelangi Foundation. A criminal justice professional interviewed expressed the view that criminal justice professionals have difficulties calculating compensation for immaterial costs (meaning costs that are not easy to quantify e.g., emotional pain and suffering). (RA4-IN-05-A-justice) Another justice professional also indicated that *"Sometimes the victim isn't even aware that they have a right to restitution."* (RA4-IN-08-A-justice)

Challenges in enforcement: Even in cases where restitution is applied for and awarded by the court, it can prove difficult to enforce. The Director of the Surabaya Children Crisis Centre explained that OCSEA offenders usually opt for longer prison sentences instead of paying restitution. The legal representative from the Centre for Study and Child Protection provided an example: *"The restitution was granted on paper but there was no implementation… the offender was not willing to pay, so the offender chose extended jail time instead because it was an option."* (RA4-IN-06-A-justice) Current legislation does not provide criminal justice professionals with mechanisms for recovering the restitution from the offender e.g., by confiscating the assets of offenders that are able but unwilling to pay. [144]

136. Government of Indonesia (2002). Child Protection Law (as amended in 2014) (Untranslated), Article 18.
137. Government of Indonesia (2002). Child Protection Law (as amended in 2014) (Untranslated), Article 64 (c).
138. Government of Indonesia (2002). Child Protection Law (as amended in 2014) (Untranslated), Article 59 (1), 69 (a).
139. Aljazeera. (2022 April 12). Indonesia passes landmark bill to tackle sexual violence.
140. For more information, see the Pusat Kajian dan Perlindungan Anak homepage.
141. For more information, see the Surabaya Children Crisis Centre webpage.
142. Government of Indonesia (2002). Child Protection Law (as amended in 2014) (Untranslated), Article 71 (d).
143. Government of Indonesia (1981). Law No. 8 of 1981 on the Code of Criminal Procedure, Articles 98-101.
144. Information provided by a representative from ECPAT Indonesia on 15th February 2022.

3.3.3 Social support services

Arrangements for social support to child victims

According to the government representatives interviewed, the Integrated Service Centres for the Empowerment of Women and Children (P2TP2As) play a central role in the provision of support services for child victims of violence including OCSEA and act as referral centres to ensure consistency of support to the victims. Though government representatives indicated that civil society organisations support the P2TP2As in providing services to children, it was also mentioned that cooperation among child protection organisations that offer the support is weak at district and sub-district levels due to the lack of resources and capacity. In addition, P2TP2As do not have their own social workers but work with volunteer staff from government departments and civil society organisations. In terms of jurisdiction, a government representative pointed out that the Integrated Service Centres for Women and Children have limited geographical jurisdiction on the cases they can handle due to the regional autonomy policy (RA1-IN-01-A&B) According to a government representative interviewed, this represents a challenge for law enforcement agencies seeking to coordinate with these centres because *"when it comes to the online-based violence like OCSEA which is borderless, the case cannot be handled only by one local government; it requires cross-provincial works."* (RA1-IN-01-A&B)

The institution of P2TP2A is however being replaced by Unit *Pelaksana Teknis Daerah Perlindungan Perempuan dan Anak* (in short UPTD PPA). While P2TP2As involve civil society organisations, the UPTD PPA structures are led and funded by local government with technical support and additional operational funds from the Ministry of Women Empowerment and Child Protection. As of March 2022, the UPTD PPA structures had not yet been established in all regions.[145]

Besides the P2TP2A and UPTD PPA, another government unit that coordinates the provision of services to child victims of abuse is the Integrated Social Welfare Centre for Children and Families (*Pusat Kesejahteraan Sosial Anak Integratif* or PKSAI). Initially piloted in 5 districts with support from UNICEF, by 2021 these centres have been expanded to more provinces and districts with funding from the Ministry of Social Affairs.[146] Integrated Social Welfare Centre for Children and Families enable access for children and families to health services, law enforcement, education and birth registration.[147] Interviews with government representatives and criminal justice professionals did not provide insight on how effective the Integrated Social Welfare Centres for Children and Families are in the provision of support services.

Cited below is the feedback given by government representatives and criminal justice professionals on specific services:

- **Medical services:** A respondent representing the Integrated Service Centre for the Empowerment of Women and Child (P2TP2A) DKI Jakarta indicated that *"We refer the victims there [to hospitals] ... After that, the victims of violence can receive priority medical services...That is the general picture for health services."* (RA4-IN-01-A-justice)

- **Recovery and rehabilitation services:** Civil society organisations assist with psychosocial support by providing counselling services to child victims, including victims of OCSEA and their families. The trafficking client's companion from the Bahtera Foundation reported that *"We provide counselling to the family and the child, continuous counselling."* (RA4-IN-04-A- justice)

---

145. This information was provided by the participants during the Disrupting Harm national consultation for Indonesia that took place in March 2022.
146. Information was provided by a representative from UNICEF Indonesia on 15th February 2022.
147. Child Frontiers (2019). Formative evaluation of the Integrated Child Welfare Program (PKSAI).

Psychosocial support from government psychologists was said to be limited due to insufficient budgetary resources. One government representative told *Disrupting Harm* that: *"The [government] budget for the psychologist or consultant is limited, so the treatment for the victim is not effective due to many problems in terms of budgeting and administrative."* (RA1-IN-01 A&B)

For rehabilitation services, a criminal justice professional commented that *"Government services such as the Ministry of Social Affairs or P2TP2A, whether at the national, provincial, or city/regency levels, do not have rehabilitation services for child victims of sexual exploitation. It is non-existent up to this point."* (RA4-IN-05-A-justice)

The interviews with criminal justice professionals revealed that there are rehabilitation centres in some places. Yet according to the Director of the Surabaya Children Crisis Centre, *"Even though there are rehabilitation and restitution centres in Surabaya, I still don't believe they are run and managed well enough."* (RA4-IN-02-A- justice)

A criminal justice professional recommended that *"Social rehabilitation process policies must be improved for child victims, so their rights are fulfilled."* (RA4-IN-08-justice) A judge of the Supreme Court also recommended that *"the government can be more assertive in practicing the laws ...[and] must not ignore the long-term recovery and rehabilitation process for children who faced the process of law."* (RA4-IN-10-A- justice)

Frontline worker perceptions of quality and availability of support services

In the survey of frontline workers undertaken by *Disrupting Harm*, the respondents were asked to evaluate the overall availability and quality of medical, psychological, legal and reintegration services for child victims of OCSEA. While the research team aimed to cover various geographical areas, the sample of providers is not representative and likely to represent services located in urban/peri-urban areas, which may affect their ratings of service quality and availability. Figures 26 and 27 below show fairly consistent ratings among all services.

Figure 26. Perception of frontline workers on the *availability* of services.
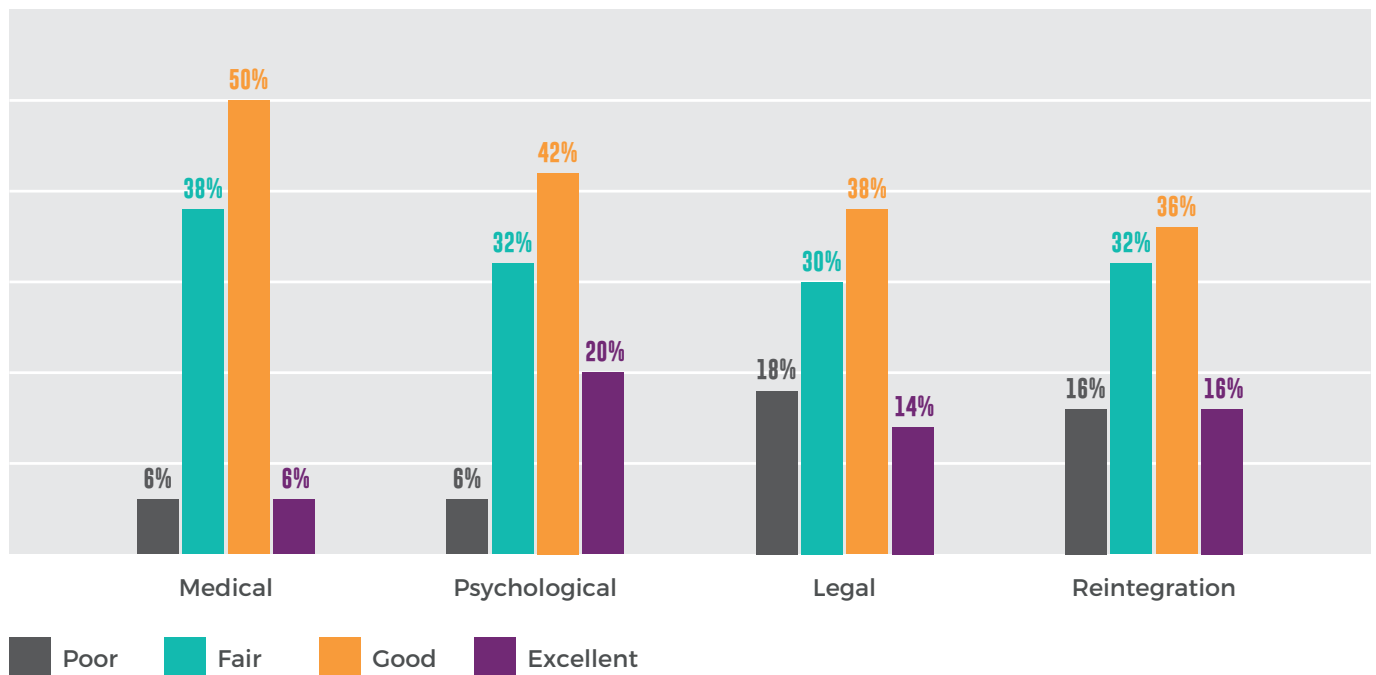
Base: Frontline workers. n = 50.

Figure 27. Perception of *Quality* of Services.

Poor ▪ Fair ▪ Good ▪ Excellent

	Medical	Psychological	Legal	Reintegration
Poor	4%	6%	24%	16%
Fair	42%	34%	20%	34%
Good	48%	48%	48%	42%
Excellent	6%	12%	8%	8%
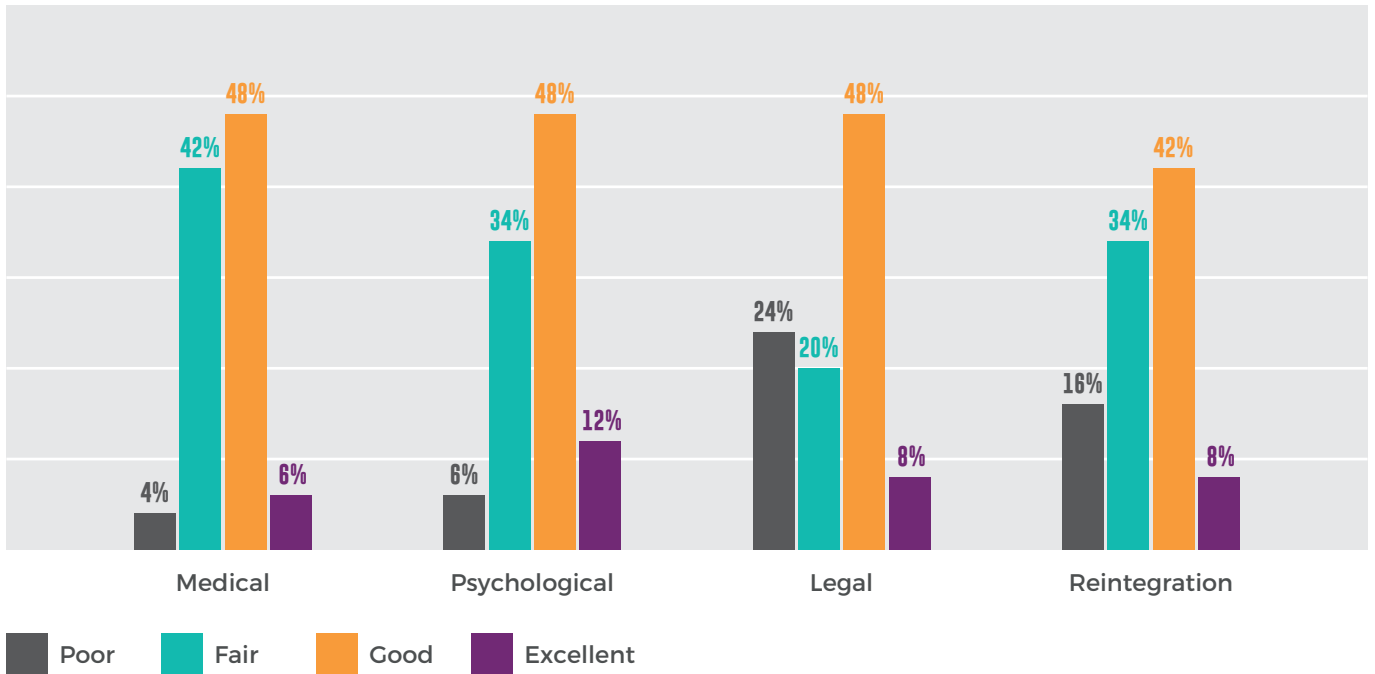
Base: Frontline workers. n = 50.

As shown in figure 28 below, the concentration of services in urban areas was ranked by three quarters of the frontline workers surveyed as the biggest factor affecting the availability of support services to child victims of sexual exploitation.

In the words of one of the frontline workers surveyed, *"There's still a lack of services that reach all areas, including rural areas."* (RA3-IN-04-A)

Figure 28: Factors affecting the availability of support services for child victims of Child sexual exploitation.

Factor	Percentage
Services concentrated in urban areas	74%
Low quality of service	54%
Cost of services	50%
Services discriminate against clients	38%
No service available	34%
Gender	32%
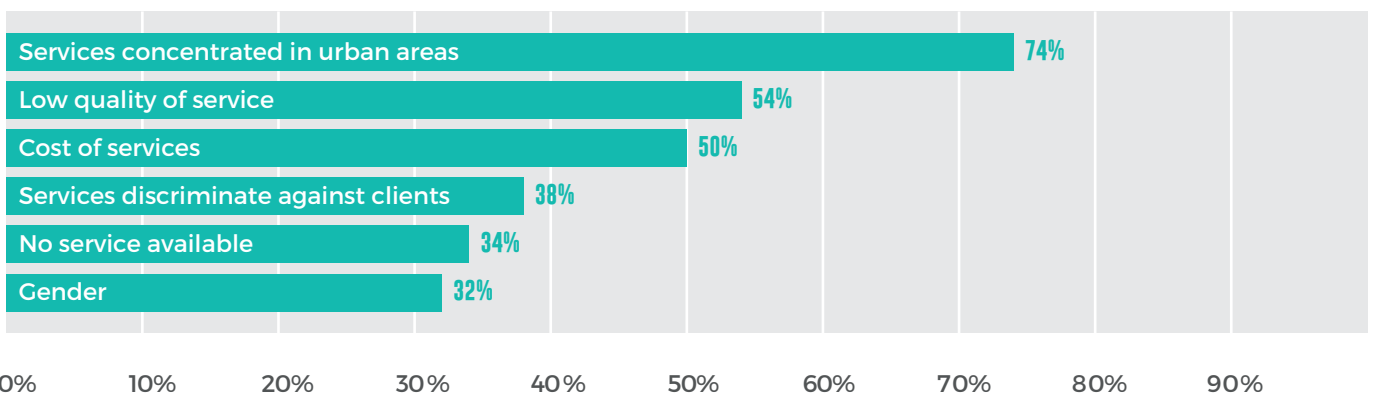
Base: Frontline workers. n = 50.

3.4 COORDINATION AND COLLABORATION

3.4.1 Policy and government

The government ministries and agencies relevant for addressing OCSEA in Indonesia include the following:

- The Ministry of Women's Empowerment and Child Protection, which has the duty of developing, adopting and coordinating policies on child protection.[148] Other duties of the ministry include coordinating implementation of child protection programmes, provision of referral services for children in need of special protection, and provision of support to Unit Pelaksana Teknis Daerah Perlindungan Perempuan dan Anak (UPTD PPA). The mandate of the Ministry of Women's Empowerment and Child Protection in addressing OCSEA is recognised by other government agencies, as is evident from a remark made by a representative of the Attorney General's Office *"Based on the Law on the Child Criminal Justice System, the Ministry of Women Empowerment and Child Protection is given the mandate. So most often we collaborate with the Ministry of Women Empowerment and Child Protection."* (RA1-IN-06-A) IN-A)

- The Ministry of Communication and Information Technology, which is tasked with the registration and licensing of electronic system operators and developing and implementing national policies related to information and technology.[149] This ministry is also the main body responsible for filtering online information, including negative content and fake news.

- The Ministry of Social Affairs, which develops and implements social rehabilitation policies including those for child victims of violence, trafficking and neglect.[150,151]

- The Ministry of Law and Human Rights, which is responsible for harmonising and drafting laws and regulations.

- The National Police of Indonesia.

In addition to the above, the following ministries are also important: the Ministry of Health, as the health system can play a vital role as the gateway to identification and support for victims, and the Ministry of Finance, as budget allocation to mandated government agencies for the implementation of OCSEA related programmes is a crucial part of the national response to OCSEA.

Government response to OCSEA

Government representatives said that although OCSEA is a rising threat in Indonesia, the government's current efforts to address it are limited. As shown below in figure 29, government efforts to raise awareness on OCSEA were rated as 'fair' by 24 out of 50, and as 'good' by 18 out of the 50 surveyed frontline workers, whereas efforts to train stakeholders on OCSEA were rated as 'fair' by 19 out of 50, and as 'good' by 20 out of the 50 surveyed frontline workers. Governments efforts to address OCSEA in general were rated by very few frontline workers as 'excellent'. This may be an indication that though there are ongoing government efforts, more still needs to be done.

While Indonesia has a strong national policy agenda to protect children, the prevention and intervention strategies do not focus heavily on child sexual abuse.[152] The 2019 midterm review of the ASEAN Regional Plan of Action on the Elimination of Violence against Children 2016–2025 also reported a lack of specific education programmes on online safety.[153]

Meanwhile, government representatives considered frontline welfare workers to have only a 'fair' understanding of OCSEA. According to one government representative, *"We have not educated the social workers about this [OCSEA]."* (RA1-IN-09-A) For this reason, government representatives argued that frontline workers rarely identify or specifically address online aspects of child sexual abuse and exploitation.

148. UNICEF (2016). Child protection in the digital age. National responses to online child sexual abuse and exploitation in ASEAN Member States.
149. Ministry of Communication and Informatics. (2017). Annual Report 2017. Jakarta: Ministry of Communication and Informatics.
150. UNICEF (2016). Child protection in the digital age. National responses to online child sexual abuse and exploitation in ASEAN Member States.
151. President of the Republic of Indonesia. (2021). Presidential Decree No. 110 of 2021.
152. Pratama, B., Sofian, A., & Talerico, C. (2018). Weighting Approaches on Online Sexual Abuse of Children: Cultural Prevention or Crime-Based Enforcement? Udayana Journal of Law and Culture, 2(2), 191-219.
153. UNICEF (2016). Child protection in the digital age. National responses to online child sexual abuse and exploitation in ASEAN Member States.

Figure 29. Front line workers' perceptions of quality of government efforts to address OCSEA.

Base: Frontline workers. n = 50.

Government representatives interviewed for *Disrupting Harm* did not know of any specific central government budget line for addressing OCSEA in Indonesia. They noted that funding for child protection in general is mostly directed to the Ministry of Women's Empowerment and Child Protection. One interviewee added that this funding *"is mostly divided into three main activities, first is for drafting policy papers, briefs, or document, the second is for coordinating activities and socialisation, third is for capacity building."* (RA1-IN-05-A)

Regarding coordination, while government representatives interviewed mentioned the existence of the Task Force for Anti-Pornography, they did not provide specific information on its effectiveness in coordinating OCSEA related initiatives.

Promising developments and initiatives
Recognition of OCSEA as an issue that needs to addressed: Despite the limited government efforts, it was evident from the interviews that the government is aware of the threat of OCSEA. As one frontline worker commented, OCSEA *"has started to be noticed by the government."* (RA3-IN-04-A)

Challenges
Data collection: Government representatives identified data collection as a challenge to combating OCSEA in Indonesia. It was pointed out that OCSEA cases are not specifically categorised and referred to as such, especially at the policy level: *"It is because the term of online child sexual abuse has not yet [been] defined in details on our RPJMN [National Medium-Term Development Plan]. In the policy paper we try to compact that issue into a more general protection issue."* (RA1-IN-05-A) A law enforcement official also told *Disrupting Harm* that the data collected by law enforcement authorities is not categorised in detail, making it difficult to identify trends relating to child sexual abuse and exploitation. (RA1-IN-01-A&B)

3.4.2 Civil society

Civil society organisations are actively involved in addressing OCSEA in Indonesia in collaboration with law enforcement and government institutions. From the interviews with government representatives and criminal justice professionals it was clear that civil society organisations are mostly involved in the provision of services, such as legal aid and psychosocial support, and collaborate with law enforcement and the Integrated Service Centres for the Empowerment of Women and Children.

3.4.3 Internet service providers and platforms

Collaboration with internet and mobile service providers and platforms is essential to investigate crimes and prevent the dissemination of CSAM. The legal requirements and practical procedures differ depending on whether the operators are Indonesian or foreign.

Domestic Internet Service Providers

Evidence gathering: Interviews with law enforcement agencies revealed that the Indonesian internet service providers share information with them when asked for. Thus, the law enforcement authorities appear to have enlisted the cooperation of domestic players in the industry.

Removing/reporting CSAM: Indonesian law does not have provisions that explicitly compel internet service providers to filter and/or block child sexual abuse material and report companies and/or individuals disseminating, trading, or distributing these materials. However, the Law on Pornography requires the government and regional governments to prevent the production, distribution and use of pornography,[154] which includes child sexual abuse materials.

In order to do this governmental and regional authorities are allowed to cut off networks of production and distribution of pornography products or pornography services, including blocking pornography through the internet, and to co-operate and coordinate with other parties in and outside of the country to prevent the production, distribution and use of pornography.[155]

A representative of the Ministry of Communication and Information Technology explained that: *"The government has the authority to terminate access or to order electronic system administrators to terminate access. For example, [if] there is content on a social media platform that violates the law, the Ministry can request for this content to be taken down. What kinds of content violate the law? … the major ones include pornography, violence, and terrorism."* The respondent further explained that *"Our law on pornography does not differentiate between child and adult pornography."* (RA1-IN-08-A)

Since 2018, the Ministry of Communication and Information Technology has been operating a Negative Content Crawling Machine, which helps to detect inappropriate content and block it from spreading further.[156] More than a million sites (mostly pornography sites) were blocked by the ministry between January and June 2019.[157]

In 2014, the Minister of Communication and Information Technology issued Regulation No. 19 of 2014 on Controlling Internet Websites Containing Negative Content.[158] The regulation provides, *inter alia*, for the establishment of a 'TRUST+ Positif List', a database of websites with negative content, including 'pornography'.[159] Government institutions, law enforcement officers and the general public may submit reports on negative content (pornographic or unlawful material) to the Director General of Information Technology via aduankonten.id, requesting it to be removed. The website is then placed on the 'TRUST+ Positif List'.[160]

154. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Article 17.
155. Government of Indonesia (2008). Law No. 44 of 2008 on Pornography, Articles 18 and 19.
156. Ministry of Communication and Informatics. (2017). Annual Report 2017. Jakarta: Ministry of Communication and Informatics.
157. Silviana, C. (2019). Indonesia will impose fines on Facebook and other social platforms due to negative content. KrASIA.
158. Government of Indonesia (2014). Regulation No. 19 of 2014 on Controlling Internet Websites Containing Negative Content.
159. The database can be accessed here.
160. Makarim & Taira, S. (2014). Indonesia: Internet content censorship strengthened in Indonesia.

The regulations oblige internet service providers to block all websites on the 'TRUST + Positif List'.[161] They are also required to maintain their databases of prohibited websites in accordance with this list and update them on a regular basis.[162] Internet service providers that fail to block websites on the list may incur administrative or criminal liabilities under Law No. 36 of 1999 on Telecommunications, Law No. 44 of 2008 on Pornography and Law No. 11 of 2008 on Information and Electronic Transactions.[163]

In 2019, the government issued Government Regulation No. 71, which authorises the government to block access to prohibited content.[164] Prohibited content includes "electronic information and/or an electronic document that contains or promotes", *inter alia*, "pornography" and violence against children. Removal of negative content is still carried out by the internet service providers; the government only asks the providers to block content,[165] and the primary responsibility for controlling online content still rests with internet service or content providers.[166]

Global platforms
Evidence gathering: Global platforms cannot be compelled to disclose information by Indonesian court orders or Indonesian authorities since they are governed by the domestic laws in their own countries – in the case of the United States, the Stored Communications Act and Electronic Communication Privacy Act. U.S. Law expressly prohibits the disclosure of communications content such as messages and images directly to non-U.S. law enforcement authorities. However, United States-based tech platforms may voluntarily disclose non-content data to foreign authorities, including subscriber data and IP logs needed for conducting investigations.

Government representatives suggested that working with international technology service providers in Indonesia is challenging. According to one, *"The worst thing is that not all platform providers have a representative office in Indonesia … There is a different policy between Indonesia and the country where the platform is from."* (RA1-IN-07-A) Another government representative added: *"To tackle the 'child pornography' issue, we still depend on international cooperation, because we do not own the platform. The server of Facebook, Twitter, and Instagram are in the United States not in Indonesia. They tend to be difficult to reach out to solve the case when it is not part of the platform's priority."* (RA1-IN-01-A&B)

Removing/reporting CSAM: With respect to removing/reporting CSAM, there are rarely any formal agreements between national law enforcement agencies and global platforms. The platforms would prefer to view requests from government partners as notifications of potential violations of their own terms of service. Since CSAM is contrary to the platforms' terms of service and U.S. law, it would be in the companies' interests to remove such content.

---

161. Government of Indonesia (2014). Regulation No. 19 of 2014 on Controlling Internet Websites Containing Negative Content.
162. Government of Indonesia (2014). Regulation No. 19 of 2014 on Controlling Internet Websites Containing Negative Content.
163. Government of Indonesia (2014). Regulation No. 19 of 2014 on Controlling Internet Websites Containing Negative Content.
164. Government of Indonesia (2019). Regulation No. 71 of 2019 on Electronic Systems, Article 95.
165. Tirto.id (March 8, 2018). Kominfo Catat 11 Medsos Punya Konten Negatif, Twitter Terbanyak
166. Song, K. (2015). Protecting Children from Cybercrime. Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying. The World Bank & International Centre for Missing & Exploited Children.

Transparency data

In 2017, 2018 and 2019, the transparency reports of major social media platforms show that authorities in Indonesia made:

- 1,043 requests to Facebook for content restriction, for reasons including anti-religious hate speech, promotion of Communist ideology, extremism, trading in endangered goods, blasphemy, defamation, violation of election blackouts, treason and separatism, and unlawful assembly;

- 232 requests for Facebook user data;

- 1,723 requests to Google for content removal, of which 226 concerned adult content, 8 obscenity/nudity and 441 violent content;

- 11 requests for Google user data;

- 38 requests to Apple;

- 69 requests to Twitter for user data, and 886 for content removal;

- 1 data request to Verizon Media

While none of the major platforms publish data specific to OCSEA or fully disaggregated by the type of crime, the diversity of platforms addressed suggests that Indonesia engages with U.S.-based technology companies more than some of the other Southeast Asian countries studied for *Disrupting Harm*.[167]

---

167. Platforms were selected on the bases of high volumes of reports to NCMEC (10,000+), availability of transparency reporting, and known popularity in *Disrupting Harm* focus countries. In addition to U.S.-based companies, transparency reports for Line and TikTok were also reviewed.

4. HOW TO DISRUPT HARM IN INDONESIA

Disrupting harm from OCSEA requires comprehensive and sustained actions from all stakeholders – families, communities, government representatives, law enforcement agencies, justice and social support service professionals, and the national and international technology and communications industries. While children are part of the solution, the harm caused by OCSEA obliges adults to act to protect them; we must be careful <u>not to put the onus</u> on children to protect themselves from harm without support.

The recommended actions below are clustered under six key insights from the *Disrupting Harm* research and signposted for different stakeholder groups. However, all these recommendations are interlinked and are most effective if implemented together.

4.1 SIX KEY INSIGHTS AND RECOMMENDATIONS FOR ACTIONS

INSIGHT 1

In the past year, at least 2% of internet-using children aged 12–17 in Indonesia were subjected to clear examples of online sexual exploitation and abuse that included being blackmailed to engage in sexual activities, having their sexual images shared without permission, or being coerced to engage in sexual activities through promises of money or gifts. This number likely reflects underreporting.

Government

1.1 Engage the public – including children, caregivers, teachers and others – in awareness of violence against children including OCSEA via existing national programmes.[168] Ensure that:

- Awareness and education programmes are evidence-based. They should be developed and tested through safe and ethical consultations with children, caregivers and teachers to ensure that they address their lived experiences of online risks and also include the techniques children use to keep themselves safe. This will help to create campaign messages that are relevant to children's lived experiences and therefore more likely to resonate with them.

- The campaigns have universal reach. Children aged 12–13 and children living in rural areas were found to be the least likely ever to have received information on how to stay safe online. Children not in school must also be reached.

- Existing evidence-based programmes that have proven to be effective are adapted and contextualised to Indonesia, prioritised and sustained.

- Interventions and programmes are monitored and evaluated, and use is made of innovative tools such as the online safety programmes evaluation model[169] recently developed by a global panel of experts on online safety. This framework of indicators was designed to address the specific challenges of the East Asia and Pacific regions.

Key objectives of awareness programmes should include:

- Making children, caregivers and teachers fully aware of the role technology might play in the sexual exploitation and abuse of children.

- Equipping caregivers with the knowledge and skills to foster safe and ongoing communication with children about their lives – both online and offline – leveraging, when possible, existing positive parenting programmes in Indonesia. Good practices exist[170] that can be built on and tailored to the local context.

- Equipping adults and children to recognise signs of potential abuse and informing them about how and where to seek help for oneself or for others.

- Fostering an environment in which children are more comfortable having conversations about sexuality or asking adults, including teachers, for advice. Feelings of discomfort, shame or embarrassment can make children reluctant to discuss sexual matters with adults: in fact, up to 37% of the children surveyed said they *did not want* to receive any sex education, which could indicate how children perceive discussing sexuality to be stigmatizing. While children should not be forced to engage in conversation, they are not comfortable with, in the context of OCSEA it would be beneficial for children if adults create an environment where children feel safe enough to report and seek help when experiencing sexual exploitation or abuse. Support for caregivers – especially older caregivers who are infrequent users of the internet or have never used the internet – in going online and becoming more familiar with the platforms that children are using.

---

168. This aligns with the ASEAN Regional Plan of Action Activity 6.2.1 on supporting mass and targeted public campaigns on online safety. *ASEAN. Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN: Supplement to the ASEAN Regional Plan of Action on the Elimination of Violence Against Children.* (forthcoming).
169. UNICEF. (forthcoming). Evaluating Online Safety: What Works to Keep Children Safe Online.
170. See: the Australian eSafety Commissioner's programme 'Start the Chat' to encourage caregivers to talk with their children about their lives online; and eSafety Commissioner's programme for seniors going online for the first time 'Be Connected'.

These messages should be disseminated via the channels preferred by the recipients:

- *Disrupting Harm* data show that schoolteachers are both the primary source and a preferred source of sex-related education or information for children. They are also one of the possible points for disclosure for a number of children. Engaging teachers in campaigns is critical not only for disseminating key messages but also for building trust and a sense of safety so as to enhance the opportunity for an open conversation and, where necessary, disclosure.

- For caregivers, the *Disrupting Harm* survey highlighted children's schools and television, as well as family or friends, as actual and preferred channels for receiving guidance on children's internet use and how to keep them safe. These channels could be leveraged to disseminate awareness messages or educational programmes on how caregivers can empower children to use the internet safely and effectively.

The suggested government body[171] that could lead in implementing this recommendation is the Ministry of Women Empowerment and Child Protection. The Ministry, supported by the Agency for Population and Family Planning, can also play a role in supporting caregivers. The Ministry of Education could lead on the training of teachers and for sexual and reproductive health education, and the Ministry of Social Affairs could create awareness through Family Development Sessions (*Sesi Temu dan Penguatan Anak dan Keluarga* or TEPAK)[172]

Awareness raising efforts are not sufficient on their own to tackle and prevent OCSEA. Instead, these initiatives should occur in tandem with other prevention efforts recommended below.

1.2 Invest in digital literacy programmes for children, caregivers and teachers.
- Provide comprehensive digital literacy and safety training to ensure that children and trusted adults are both *aware* of possible risks and know what to do about them. Forty-one percent of children surveyed have never received information on how to stay safe online. This should include information about what children can do if they are being bothered online, what kind of content is appropriate to share online with others, and basic skills such as how to change their privacy settings and block people from contacting them.

- Integrate cyber safety education into school curricula and empower teachers to guide children's internet use.

- Ensure that these programmes reach younger children and children in rural areas, who have the lowest rates of risk awareness and digital skills, as well as children not in school.

- Provide additional support to older caregivers, many of whom have never used the internet.

- Integrate digital literacy information into positive parenting programmes.

1.3 Increase coordination and cooperation across programmes focused on online versus offline violence and, to the extent that it proves appropriate, across programmes focusing on violence against women and children.

Caregivers, teachers and social support services[173]

1.4 Engage with children to encourage open dialogue about their online and offline interactions and behaviour. Become informed about current and emerging risks to children. Be aware that in Indonesia, the evidence suggests that boys and girls are equally likely to report having experienced OCSEA. Free and publicly available resources and guidance on digital literacy are made available by the Ministry of Communication and Informatics.[174]

---

171. The recommendations for the leading organisations and bodies are based on discussions with over 97 participants – from government, law enforcement, civil society and non-governmental organisations – at the national consultation for the *Disrupting Harm in Indonesia* report.
172. The Family Development Sessions (*Sesi Temu dan Penguatan Anak dan Keluarga* or TEPAK) can be expanded to create awareness for families who receive cash support for social protection programme which include children in need of special protection and parents/caregivers of the children. Intel Resos. Rehabilitasi Sosial Anak.
173. Government, intergovernmental agencies, and civil society need to translate and convey these messages to reach caregivers, teachers and social support staff.
174. See resources from the Ministry of Communications and Informatics here.

INSIGHT 2

According to the household survey, OCSEA offenders are most often people already known to the child – often an adult friend, a peer or a family member.

Government

2.1 Implement programmes that cover comprehensive sexuality education. Seventy-two percent of children surveyed in Indonesia have not received any comprehensive sex education.

- Programmes should cover issues such as sex, consent, personal boundaries, what adults or others around children can or cannot do to them, risks and responsibilities when taking, sending and receiving sexual images, and how to say 'No' to others.

- As schoolteachers are a preferred source of sex education, they should receive additional training on OCSEA. The existing school curriculum should be scaled up at all levels, building on international guidance such as the WHO Comprehensive Sexuality Education guidelines[175] and adequate resources should be allocated for implementation.[176] Information on sexuality, sexual health and OCSEA could also be integrated into existing violence prevention programmes in schools (e.g., The Roots Programme[177]).

2.2 Age-appropriate and gender-sensitive education and awareness raising approaches need to reach all children in Indonesia. Younger respondents were consistently the least likely to recognise the risks associated with potentially harmful online activities. Although it might be uncomfortable to discuss these issues with younger children, they should also be included in these awareness efforts. Special care should also be taken to ensure that information is communicated to children whose situation may increase their vulnerability to OCSEA, including children with disabilities, children engaged in migration, street-connected children, out-of-school children, and children who experience other forms of violence.[178] Civil society organisations may be ideally positioned to deliver information to these vulnerable populations. This is not intended to place the burden on children to protect themselves, but rather to help them become aware of the risks.

There are other existing reports[179] and initiatives[180] developed internationally that might act as helpful references and good practice examples of age-appropriate resource material.[181]

2.3 Develop programmes to guide those with a duty of care for children – caregivers, teachers, medical staff, etc. – on violence prevention. Where possible, incorporate this into existing teacher trainings or parenting programmes. These programmes should encourage positive adult-child interaction to overcome discomfort in discussing sex and sexuality in age-appropriate terms. This can encourage open dialogue about sexual abuse and exploitation online or in person.

175. UNESCO, UNAIDS, UNFPA, UNICEF, UN Women and WHO. (2018). International technical guidance on sexuality education: An evidence-informed approach.
176. Susanti, D. & Doni, A. (2021). Implementation of Sexual Education Programs for Adolescents in Indonesia: Narrative Review. SANITAS: Jurnal Teknologi Dan Seni Kesehatan, 12(1), 36-52.
177. The Roots Program is an evidence-based intervention model that has been developed to prevent bullying in schools by involving students as agents of change to help create a positive climate in schools.
178. This aligns with the ASEAN Regional Plan of Action Activity 1.3.3 to ensure that the specific needs of vulnerable groups are appropriately integrated in the development and implementation of national policies and programs aimed at tackling OCSEA, and Activity 6.2.2: to ensure targeted awareness raising and digital literacy interventions for all vulnerable children and high-risk groups.
179. UNFPA. (2021). My Body is My Own.
180. UNGEI. (2020). Bodily autonomy and SRHR.
181. National Society for the Prevention of Cruelty to Children. (2017). Talk PANTS with Pantosaurus and his PANTS song #TalkPANTS – YouTube. While Pantosaurus does not specifically say offenders can be people you know, he gives basic rules that apply to every time someone (anyone) crosses these boundaries.

In the longer term, this will make it easier for caregivers to talk to and support their children and will make children more likely to come to their caregivers to seek support when needed. Guidance and skills-building for teachers and caregivers could be provided through existing government interventions and programmes, including positive parenting programmes (e.g., Center for Family Learning (PUSPAGA) or the UNICEF *Creating Connection* Module).

Several guidelines exist, including a parent guidance developed to support the implementation of parenting interventions that prevent and respond to violence against children.[182]

As they may act as an important point of contact for children who disclose situations of sexual abuse, guidance and training should also be provided to social support workers to recognise exploitative or abusive behaviour. Social support workers may also be involved in the delivery of awareness messages to children, including in schools (e.g., Sakti Peksos *Goes to School* programme)[183] and as such should be trained on the nature and signs of OCSEA. Information about OCSEA could be integrated in training modules on Child Protection Service Standards delivered to social workers by the Ministry of Women Empowerment and Child Protection.

Information and support can be disseminated to the wider community through Family Welfare Programme (Programme *Kesejahteraan Keluarga* or PKK) organisations,[184] Children's Forums, Youth Organizations, and Community-based Integrated Child Protection Mechanism (*Perlindungan Anak Terpadu Berbasis Masyarakat* or PATBM).[185]

2.4 Engage with owners and proprietors of internet cafes and other computer rental shops to ensure adequate safeguards are in place and as avenues to promote information among children about online safety strategies, help-seeking and reporting mechanisms, and practices that promote positive engagement with digital technologies.

Caregivers, teachers and social support services[186]

2.5 Inform children about their right to be protected from all forms of emotional, physical and sexual abuse and exploitation, including OCSEA. This could include information on how to stay safe by setting boundaries, recognising appropriate and inappropriate behaviour and knowing how to say 'No' to inappropriate behaviour. Education and awareness-raising efforts should not focus disproportionately on 'stranger danger'. Data suggest that offenders tend to be people known to the child, at times family members. Children should be made aware that all forms of sexual exploitation and abuse (both online and in-person) are unacceptable, even if committed or facilitated by family members or trusted adults.

2.6 Facilitate access to trusted online sources of information for children as a complement to adult-led comprehensive sexuality education.[187] Children may be reluctant to seek sex-related information and advice from adults and may rely on their peers (91% of children surveyed said they could talk to their friends about their problems) or may resort to seeking answers online. Social workers, teachers and other trusted adults should promote reliable online sources of information – such as the mobile apps *Unala*[188] or *Springster*[189] – among children.

182. Landers, C. et al. (2020). Designing Parenting Programmes for Violence Prevention: A Guidance Note. UNICEF.
183. Social Workers' Child Service Unit (Satuan Bakti Pekerja Sosial Anak) *Goes to School* is a violence prevention program implemented by the Ministry of Social Affairs targeting middle and high school students in 806 locations in Indonesia. This capacity building program concerns issues such as prevention of online sexual abuse, anti-bullying de-radicalisation.
184. PKK is based on New-Order (1965 – 1998) regime approach, in which key government programme priorities are implemented by women's groups at village level. The key focuses are 10 programmes to strengthen families and communities, including on education.
Depending on the support from local government and the use of village-fund, the PKK cadres can be effective in addressing child protection issues through parenting initiatives.
185. Community-based Integrated Child Protection Mechanism (*Perlindungan Anak Terpadu Berbasis Masyarakat* or PATBM) was initiated by the Ministry of Women Empowerment and Child Protection and implemented by district/municipality departments of Women Empowerment and Child Protection at village level. In some villages or districts, PATBM are strong and engage in prevention and reporting of violence against children.
186. Government, intergovernmental agencies, and civil society need to translate and convey these messages to reach caregivers, teachers and social support staff.
187. United Nations Children's Fund. (2019). The Opportunity for Digital Sexuality Education in East Asia and the Pacific. Bangkok: UNICEF East Asia and Pacific.
188. This Indonesian app provides articles on sexual and reproductive health and assists teenagers in making appointments to see a doctor or counsellor.
189. Coming to life via a website, social media and an AI-powered chatbot called 'Big Sis', Springster equips girls with the knowledge, confidence and connections they need to navigate the complex choices of adolescence.

The suggested bodies that could, in synergy, lead in implementing these recommendations are the Ministry of Women Empowerment and Child Protection, the Ministry of Education and Culture and the Ministry of Communications and Informatics. Implementation could be supported by local governments at provincial, regency and city levels with the involvement of relevant Provincial/District/Municipality Technical Implementation Units for the Protection of Women and Children (Unit *Pelaksana Teknis Daerah Perlindungan Perempuan dan Perlindungan Anak* or UPTD PPA) and also by community and children's organisations groups at village level, such as the Family Welfare Programme (Programme Kesejahteraan Keluarga or PKK), the Community-based Integrated Child Protection Mechanism (*Perlindungan Anak Terpadu Berbasis Masyarakat* or PATBM), and the Children's Forum (involvement of networks that have been working on this issue).

INSIGHT 3

Children who were subjected to OCSEA on social media mainly said this happened through major platforms such as WhatsApp, Facebook and Facebook Messenger.

Government

3.1 Consult with Internet service providers, law enforcement, privacy experts, and the technology companies to develop realistic, mandatory regulations for filtering, removing and blocking CSAM addressing grooming and live-streaming of child sexual abuse, and complying with lawfully approved requests for user information in OCSEA cases. Monitor for timely compliance and implement consequences for failure to comply.

3.2 Promote awareness of OCSEA among relevant private sector entities including internet, mobile and financial service providers to ensure companies of all sizes have a better understanding of the risks children face and what they can do to combat OCSEA. Promote multi-sectoral initiatives, to develop and/or strengthen internal child protection policies

3.3 In line with the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN, ensure that the Indonesian Financial Transaction Reports and Analysis Center incorporates into existing legal frameworks with financial institutions a legal duty for them to report suspicious transactions that might involve CSAM or live-streaming of child sexual abuse.

3.4 Make it mandatory for online platforms to have clear and accessible mechanisms for children to report concerns. These platforms should detail in child-friendly language what the process looks like *after* children make a report.

The suggested bodies that could lead in implementing these recommendations are the Ministry of Women Empowerment and Child Protection, which can lead the overall coordination, and the Ministry of Communication and Information Technology, which can lead in the adoption of new policies and the enforcement in relation to the industry.

Law enforcement

3.5 Liaise more closely with global technology platforms and build on existing collaborative mechanisms to ensure that the digital evidence needed in OCSEA cases can be gathered rapidly and efficiently, including in response to data requests, and illegal content is promptly removed.[190]

Industry

3.6 Improve cooperation between Internet service providers[191] and law enforcement agencies by:

- Creating pathways for processing requests and collaborations.
- Training staff to respond to data requests for ongoing cases and minimising processing times.
- Providing the law enforcement authorities with any associated information they have that might help to identify offenders and victims in a timely manner.
- Detecting and removing OCSEA-related content on their servers.

3.7 Make formal reporting mechanisms within social media and instant messaging platforms clear and accessible to children and detail in child-friendly terms what happens after children submit a report. Platforms and internet service providers must respond rapidly to reports made by children and demonstrate transparency and accountability.

Data show that the large majority of children do not report negative experiences through an online function.

3.8 Engage with relevant governmental agencies to enhance staff training on child online protection and reporting of OCSEA.

3.9 Enhance collaboration with government and non-government agencies in building preventive measures with the engagement of the public and strengthen the development of innovative technological solutions to tackle OCSEA.

3.10 Prioritise children's needs in product development processes. Such design must be informed by evidence on children's digital practices and their experiences of online child sexual exploitation and abuse, including this *Disrupting Harm* study.[192]

3.11 Technology companies and online financial providers should consider proactively detecting and eliminating CSAM, identifying grooming attempts and live-streamed child sexual abuse utilising technology tools, such as PhotoDNA[193] or API Arachnid.[194] This is in addition to implementing the standards set out in Regulation No. 19 of 2014, issued by the Minister of Communication and Information Technology, to actively block websites with inappropriate content that children might encounter online, particularly on social media platforms. Half of the children in Indonesia who saw sexual content by accident in the past year came across it on social media (38%).

3.12 Prioritise responding to data requests from the courts, in cases involving children to help reduce the duration of trials. This could be done by having Internet service providers appoint a law enforcement liaison officer to be responsible for handling any data requests from law enforcement agencies to speed up the investigation and prosecution of OCSEA cases.

---

190. This aligns with the ASEAN Regional Plan of Action Activity 1.2.4: ASEAN Member States will endeavour to establish a legal requirement for private sector companies to report and remove CSAM from their platforms and services when they become aware of it; and for financial institutions to report suspicious transactions that may be related to CSAM or live streaming. ASEAN Member States will endeavour to impose criminal and civil liability and penalties for non-compliance.

191. This aligns with the ASEAN Regional Plan of Action Activities 7.1 - 7.5 on engaging with the private sector to identify and remove online risks to children, including the active removal and reporting of CSAM and the identification of financial interactions that involve suspected purchases of CSAM and live streaming of child sexual exploitation.

192. A good starting point for exploration are the free tools made available by the Australian eSafety Commissioner as well as well as this framework developed by UNICEF.

193. Microsoft, PhotoDNA.

194. API is the acronym for Application Programming Interface, which is a software intermediary that allows two applications to talk to each other. Mulesoft. What is an API (Application Programming Interface)?

INSIGHT 4

Children who were subjected to OCSEA tended to confide in people within their interpersonal networks, particularly their friends and siblings. Helplines and the police were almost never avenues they sought help.

Government

4.1 Given that children rely heavily on their interpersonal networks for support, especially friends, consider expanding programmes which promote dialogue amongst young people and encourage peers to seek help for abuse.

Existing initiatives such as the Ministry of Women's Empowerment and Child Protection's Children's Forums, through which children act as pioneers in prevention and as reporters of violence against children (*Pelopor Dan Pelapor* – "2P") in their regions, should be leveraged to include OCSEA.

4.2 Raise awareness that existing helplines – SAPA 129 and TePSA – can be a source of information about how to support young people subjected to OCSEA. *Disrupting Harm* data shows that children prefer to tell people that they know and trust about OCSEA. Awareness raising efforts can communicate that peers, siblings, caregivers and teachers can find information, support services and help through helplines. An important prerequisite is that helplines are adequately resourced and trained about OCSEA so that they may provide good quality information and advice.

4.3 Dedicate resources to child helplines and CSAM hotlines to improve record keeping so that they can encode detailed statistics on the OCSEA reported. Increasing the capacity of these organisations to collect and analyse such data will provide a better understanding of children's experiences of OCSEA, including how it changes over time, which could help develop prevention programmes and necessary policies and legislative amendments. Data collected could be linked to Primero,[195] which is open-source software platform that helps social services, humanitarian and development workers manage protection-related data, with tools that facilitate case management, and incident monitoring. The Primero is integrated into the *Sistem Informasi Online Perlindungan Perempuan dan Anak* (SIMFONI PPA), which is an application system for recording and reporting violence against women and children, developed by the Government of the Republic of Indonesia through the Ministry of Women's Empowerment and Child Protection. This system can be accessed by all service units handling victims of violence (women and children) at the national, provincial, and district/city levels.[196]

Caregivers, teachers, medical and social support services[197]

4.4 Foster an environment where children are comfortable seeking advice, help and conversations about sex, sexuality and reproductive health. Norms that limit discussions about sex, or that cause children to feel embarrassment and shame when they are subjected to child sexual exploitation and abuse, hinder help-seeking.

195. Primero (2021) Primero™ is putting children first Primero
196. Kemeniterian Pemberdayaan Perempuan dan Perindungan anak Republik Indonesia (n.d) Selamat Datang, SIMFONI PPA (Sistem Informasi Online Perlindungan Perempuan dan Anak)
197. Government, intergovernmental agencies, and civil society need to translate and convey these messages to reach caregivers, teachers, medical and social services.

4.5 Responses to disclosures of OCSEA should always convey that the abuse is never the child's fault, whatever choices they have made. It is always the fault of the abuser or exploiter of the child.

Data from the household survey showed that 76% of children and 85% of caregivers believed that it is the victim's fault when a self-generated image or video is shared further. Reasons commonly cited by children for not disclosing instances of OCSEA included feeling they had done something wrong or fear of getting into trouble, or of creating trouble for the family.

All responses to and interactions with children impacted by OCSEA should be without judgement or punishment.[198]

4.6 Avoid restricting children's internet access as a response to potential harm. Over half of caregivers surveyed in Indonesia said they would restrict their child's internet access if he/she was upset by something online. This can have a negative impact on children's digital skills and might be perceived by children as punishment and so reduce the likelihood of them disclosing such matters in future.

4.7 Help children, caregivers, teachers, and those working with children to understand the risks involved in sharing sexual content online, including the possibility of the content being shared further and of sexual extortion. Only 1% of children in the household survey said they had shared sexual images of themselves online, but 15% – and 27% of 12–13 year-olds – did not regard this as 'very risky'.

Law enforcement

4.8 Clearly define the mandates and responsibilities of the dedicated unit within the Cybercrimes Criminal Investigation Division for addressing cases of OCSEA. Once these are defined, strengthen their capacity and cooperation by facilitating widespread training for law enforcement officers (including at the local level). This should be supported with resources, both human and financial, so that children and families are comfortable reporting abuse. Enhance existing child-friendly procedures to ensure the best interest of the child and protect their right to be heard and informed when involved in criminal proceedings.

4.9 Establish clear guidelines on case referrals between agencies involved in case investigation. Make sure the referral of OCSEA cases aligns with the Child Protection Standard Operating Procedures, which define the role and responsibilities of child protection agencies. Establish a monitoring system to make sure the guidelines are followed.

4.10 Improve data collection and the monitoring of OCSEA cases at both the national and local levels. Systematic recording and classification of cases by law enforcement agencies will support the development of evidence-based prevention and response mechanisms. It is advised to identify and record OCSEA indicators, i.e., every case with an online element. Link OCSEA data with PRIMERO and the SIMFONI PPA (*Sistem Informasi Online Perlindungan Perempuan dan Anak*) (referred to also in rec 4.5).

---

198. See for example, World Health Organization (2019). WHO Guidelines for the Health Sector Response to Child Maltreatment.

4.1 SIX KEY INSIGHTS AND RECOMMENDATIONS FOR ACTIONS

Disrupting Harm Alignment with the Model National Response and the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN

Many countries, companies and organisations have joined the WePROTECT Global Alliance to prevent and respond to OCSEA. As a member of the Global Alliance, Indonesia can use the Model National Response to Preventing and Tackling Child Sexual Exploitation and Abuse to help organise its response to OCSEA. This model is a valuable tool for governments to organise and improve the level of their response. Most of the recommended actions in this report align with the 21 'capabilities' articulated in the Model National Response, but *Disrupting Harm* identifies priority areas for interventions based specifically on the data about the situation in Indonesia. The evidence from Indonesia shows that even though many of the capabilities in the Model National Response exist, they are not functioning optimally. The *Disrupting Harm* recommended actions primarily address legislation,[199] dedicated law enforcement,[200] judiciary and prosecutors,[201] and education programmes.[202]

All recommended actions are practical, evidence-based and actionable. *Disrupting Harm* has also indicated to whom its various recommended actions are addressed – i.e., government duty-bearers, law enforcement authorities, justice professionals, the internet and technology industries, or caregivers, the community and teachers.

The Association of Southeast Asian Nations (ASEAN) recently endorsed the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN.[203] This Action Plan includes commitments for member states to strengthen online child protection in the region. The plan has seven focus areas, ranging from awareness raising and strengthening data collection to legislative reform. The actions recommended by *Disrupting Harm* constitute sustained, practical and evidence-based activities that can be implemented in Indonesia as part of its commitment to this Regional Plan of Action.

199. Model National Response #3.
200. Model National Response #4.
201. Model National Response #5.
202. Model National Response #13.
203. Association of Southeast Asian Nations. (2020). Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN: Supplement to the ASEAN Regional Plan of Action on the Elimination of Violence Against Children.

INSIGHT 5

The mandated government agencies in Indonesia acknowledge that OCSEA is a threat, but government efforts to address it need to be more extensive. The capacities of law enforcement agencies, justice professionals and social support workers to provide victims of OCSEA with access to child-friendly justice and support services is limited by low levels of awareness of OCSEA, insufficient human and budgetary resources and inadequate technical knowledge and skills.

Government

5.1 Enhance the capacities of child protection stakeholders at district and sub-district levels, and foster cooperation among them, to provide services to OCSEA victims. Interviews with government representatives suggest that cooperation among the child protection actors that provide services for victims of violence including OCSEA at the district and sub-district levels is still weak due to lack of resources and capacity. Building their capacity and streamlining processes, sharing information and resources and minimising the duplication of efforts would improve the response to OCSEA. Participants of the national consultation for *Disrupting Harm*[204] also pointed out that there are UPTD PPAs which are responsible for service provision for child victims of violence at district level, however, these structures have limited human resources especially in remote areas.

5.2 Invest in building the technical knowledge of police officers, prosecutors, judges, lawyers, courtroom staff, child protection officers and frontline social workers, including those in remote regions, both about OCSEA and on child-friendly standards. Considering the rapidly evolving online tools and opportunities, it is essential for professionals to understand and know how to address OCSEA within their respective professions individually and as a community. These capacity-building initiatives should be institutionalised as part of the training calendar of the Government of Indonesia, to ensure necessary resources are secured and a regular and recurring budget is allocated, departing from an overreliance on sporadic foreign collaboration/ funding. The National Cyber and Crypto Agency can include this in the curriculum for digital literacy. The suggested bodies that could lead in implementing these recommendations are the Ministry of National Development Planning, which can lead in ensuring that OCSEA is a priority when developing government workplans – not only at the national level but also at the sub-national level, and the Ministry of Women Empowerment and Child Protection, which can lead the capacity building of service providers.

5.3 Increase access to, and the availability of, support services for victims of OCSEA by investing in government-run recovery and rehabilitation services instead of relying on civil society organisations. Interviews with criminal justice professionals revealed that government psychologists are often unavailable.

5.4 Standardise the implementation of child friendly approaches towards child victims of OCSEA by criminal courts in Indonesia by ensuring that all criminal justice professionals, including those in more remote regions, possess the required awareness and training. Interviews with criminal justice professionals suggest these approaches are not always implemented by courts in remote regions.

---

204. The national consultation for *Disrupting Harm* for Indonesia took place on 17th March 2022 and was attended by mandated government agencies, law enforcement representatives and civil society organisations.

5.5 Increase the number of judges, prosecutors, law enforcement officers and social workers who specialise in handling children's cases within the criminal justice system. Interviews with criminal justice professionals and government representatives suggest that there may be fewer criminal justice professionals specialising in children's cases relative to the volume of children's cases, which is one reason why OCSEA investigations and trials are protracted.

Social support services

5.6 Train all staff working in social support services (not just specialist services) to recognise the unique risks and harms of OCSEA and provide them with evidence-based best practices for responding. The training should be standardised to ensure quality and a budget allocated to make it possible. This could be done by incorporating information on OCSEA into the existing child protection social services training. When children are brave enough to seek help, those they seek help from must be equipped to provide it.

Law enforcement

5.7 Allocate sufficient human and financial resources to enable technology to be used for triage and investigation of OCSEA and to enhance preparedness and strengthen the response to this crime area.

5.8 Provide the Digital Forensic Unit team with specific capacity building on victim identification so that they can utilise the connection to INTERPOL'S International Child Sexual Exploitation database and actively engage in investigation and victim identification. Streamline workflow and responsibilities so that law enforcement authorities can respond to the high volume of CyberTipline reports.

5.9 Designated investigation officers require appropriate knowledge and skill-based training. Such training should be implemented for officers across provinces, cities municipalities, districts and police academies. This is particularly important in the remote archipelago of islands where OCSEA is also known to take place.

5.10 Establish standard operating procedures to streamline and standardise recruitment, retention and succession planning among law enforcement personnel. This would strengthen the police response to OCSEA by maintaining a critical mass of appropriately trained staff to undertake investigations and resolve cases.

5.11 Establish a data management system for OCSEA offenders and systematically track and record their movements within the country and beyond.

5.12 Promote the implementation of child-friendly procedures during the investigation process in line with the Law on the Child Criminal Justice System (*UU Sistem Peradilan Pidana Anak*).

5.13 Consider re-connecting to INTERPOL's International Child Sexual Exploitation database in order to join a community of law enforcement officers from 67 member countries working to reduce duplication of efforts, promote international cooperation and ensure effective responses.

5.14 Invest in resources to conduct proactive investigations of OCSEA. Interviews with law enforcement suggest that law enforcement units tend to be largely reactive rather than proactive and often depend on other government agencies.

Justice professionals

5.15 Expedite criminal procedures by training more criminal justice professionals to handle children's cases and to identify and address any other aspects of the criminal justice system that lead to prolonged investigations and trials in OCSEA cases.

5.16 Ensure that criminal justice professionals have a standard information package to provide to all victims and their caregivers related to child sexual exploitation and abuse (including OCSEA). The package should inform them clearly about their rights, including their right to compensation, and familiarise them with the procedures they will encounter. This will enable child victims and their caregivers to make informed decisions.

5.17 Develop and implement programmes that prepare child victims for court proceedings and provide them with adequate legal assistance to engage with the court system and legal actors, in line with the Law on the Child Criminal Justice System. Involve multi-disciplinary teams in this process.

5.18 Prevent the re-traumatisation that occurs when victims are repeatedly summoned to provide information during investigations and exposed to the offender during trials. Criminal justice professionals indicated that victims sometimes have to go back and forth to the police to provide information and do not have the option of testifying in court through video links.

5.19 Ensure victims are informed of their right to apply for protection from the Victims and Witness Protection Agency and that this protection is applied for when needed. Strengthen the capacity (human and financial resources) of the Victim Protection Agency and expand the geographical coverage of this agency so it can provide the required support to victims that apply for protection.

5.20 Ensure that child-friendly procedures are implemented whenever children are involved as victims in the justice system through the wider dissemination of training, guidance and good practices and the provision of the necessary resources. The court methods used in the Barnahus[205] model may also be explored for adoption.[206]

INSIGHT 6

Although existing legislation, policies and standards in Indonesia include provisions relevant to OCSEA, further legislative action is needed to criminalise all OCSEA-related acts.

Government

6.1 Amend legislation regarding age of sexual consent to ensure that boys and girls are treated the same, and consider a close-in-age exemption to protect adolescents from prosecution for willing sexual interactions between close-in-age peers.

6.2 Consider amending legislation in line with the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN and with international conventions that offer good guidance for addressing OCSEA, such as the Council of Europe's Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) and the Convention on Cybercrime (Budapest Convention). These conventions provide useful measures of national legal frameworks related to OCSEA and are open for accession by states that are not members of the Council of Europe.

6.3 Explicitly criminalise specific OCSEA-related crimes, such as live-streaming of child sexual abuse, online sexual extortion and online grooming for sexual purposes, and amend the legislation on CSAM to explicitly cover knowingly attending pornographic performances involving children. The Ministry of Law and Human Rights could take the lead on this, supported by other relevant Ministries, especially the Ministry of Communication and Information as well as the Ministry of Women Empowerment and Child Protection.

6.4 Amend national legislation to explicitly recognise extraterritorial jurisdiction over child sexual exploitation when this is committed by habitual residents, or when such crimes are committed against victims of Indonesian nationality.

---

205. The Barnahus model is a standard practice for providing child victims and witnesses of violence rapid access to justice and care.
206. The Barnahus model brings together the professionals in one location - including police, social workers, legal staff and others - to ease the burden on children accessing different services.

ACKNOWLEDGEMENTS